ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ РОЗПОДІЛЕНОГО ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА НА БАЗІ VMWARE NSX»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Колотухін Д.В.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВМ – віртуальна машина

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ЦОД – центр обробки даних

APIs – Application Programming Interfaces

APT – Advanced Persistent Threat

DFW – Distributed Firewall

DMZ – Demilitarized Zone

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPS – Intrusion Prevention System

IPsec – IP security

NTA/NDR – Network Traffic Analysis/Network Detection and Response

SaaS – Software as a Service

VDI – Virtual Desktop Infrastructure

VPN – Virtual Private Networks

ВСТУП

Актуальність дослідження. Сьогодні підприємства широко застосовують інформаційні технології для підвищення ефективності свого бізнесу. Треба передбачати можливий вплив зловмисників та вживати заходів підвищення безпеки інформаційних систем підприємств та організацій.

Дана проблема ще більш загострюється у сьогоднішніх умовах пандемії COVID-19, коли значна частина підприємств перейшла на відділену роботу працівників-користувачів їх інформаційних систем.

Для виявлення несанкціонованого доступу до інформаційної системи підприємства та протидії йому використовують систему виявлення та запобігання вторгненням (Intrusion Prevention System, IPS). Вважається, що система IPS має бути обов'язковою для сучасних компаній, що працюють з цифровими даними і піклуються про безпеку інформації. Вона відстежує активність в мережі в реальному часі і швидко вчиняє дії по запобіганню атак ззовні.

Системи IPS доповнюють міжмережеві екрани, захист інформації в яких відбувається шляхом обмеження трафіку з певними властивостями для запобігання зовнішніх вторгнень. IPS аналізує трафік та реагує при виявленні підозрілої активності. Ці технології доповнюють один одного, створюючи потужний бар'єр на шляху зловмисників.

Від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів виявлення та попередження вторгнень та ефективного їх застосування залежить ефективність забезпечення кібербезпеки інформаційних систем підприємства.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження методів та засобів виявлення та попередження вторгнень в інформаційну систему підприємства..

Об’єкт дослідження – захист інформаційної системи підприємства.

Предмет дослідження – технологія виявлення та попередження вторгнень в

інформаційну систему підприємства.

Мета роботи – розробити порядок застосування технології виявлення та попередження вторгнень в інформаційну систему підприємства на базі VMware NSX distributed IPS та рекомендації щодо її застосування.

Наукові завдання:

проаналізувати проблему захисту інформаційних систем підприємств;

визначити зміст проблеми виявлення та попередження вторгнень в інформаційну систему підприємства;

дослідити існуючі методи та засоби виявлення та попередження вторгнень в інформаційну систему підприємства;

розглянути порядок втілення та застосування системи виявлення та попередження вторгнень в інформаційну систему підприємства;

розробити рекомендації щодо виявлення та попередження вторгнень в інформаційну систему підприємства.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо виявлення та попередження вторгнень в інформаційну систему підприємства.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2021 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА

1.1. Аналіз проблеми захисту інформаційних систем підприємств

Розглядаючи різновиди дії загроз можна глибше вивчити інструментарій зловмисника. Рис. 1.1 дає уявлення про те, які дії призводять до збільшення кількості інцидентів, і, що здивовує, відмова в обслуговуванні (DoS) відіграє велику роль. Ми також бачимо чимало фішингу, але, оскільки розкриття даних не може бути підтверджено, вони залишаються інцидентами і не переходять до статусу порушення (але, можливо, вони зможуть це зробити). На шостому місці ми бачимо, з'являються програми-вимагачі, які в багатьох випадках досягають своєї мети [1].

Якщо розглядати основні варіанти дій для зломів на рис. 1.1, ми побачимо таких лідерів: фішинг, використання вкрадених облікових даних і неправильну конфігурацію в першій п'ятірці. Неправильна доставка показує вражаючі результати (в основному документи і електронна пошта, які були відправлені не тим одержувачам) [1].

На рис. 1.2 представлений огляд ландшафту активів. Сервери є явними лідерами і вони продовжують рости. Це в основному пов'язано з переходом підприємств та організацій до використання веб-додатків з системними інтерфейсами, наданими у вигляді програмного забезпечення як послуги (SaaS) [1]. Людина займає друге місце, що не дивно, враховуючи, наскільки соціальні дії залишалися актуальними протягом усього періоду. Кіоски і термінали продовжували знижуватися, як і в минулому році. В першу чергу це пов'язано з тим, що зловмисники переходять на роздрібну торгівлю без карти [1].

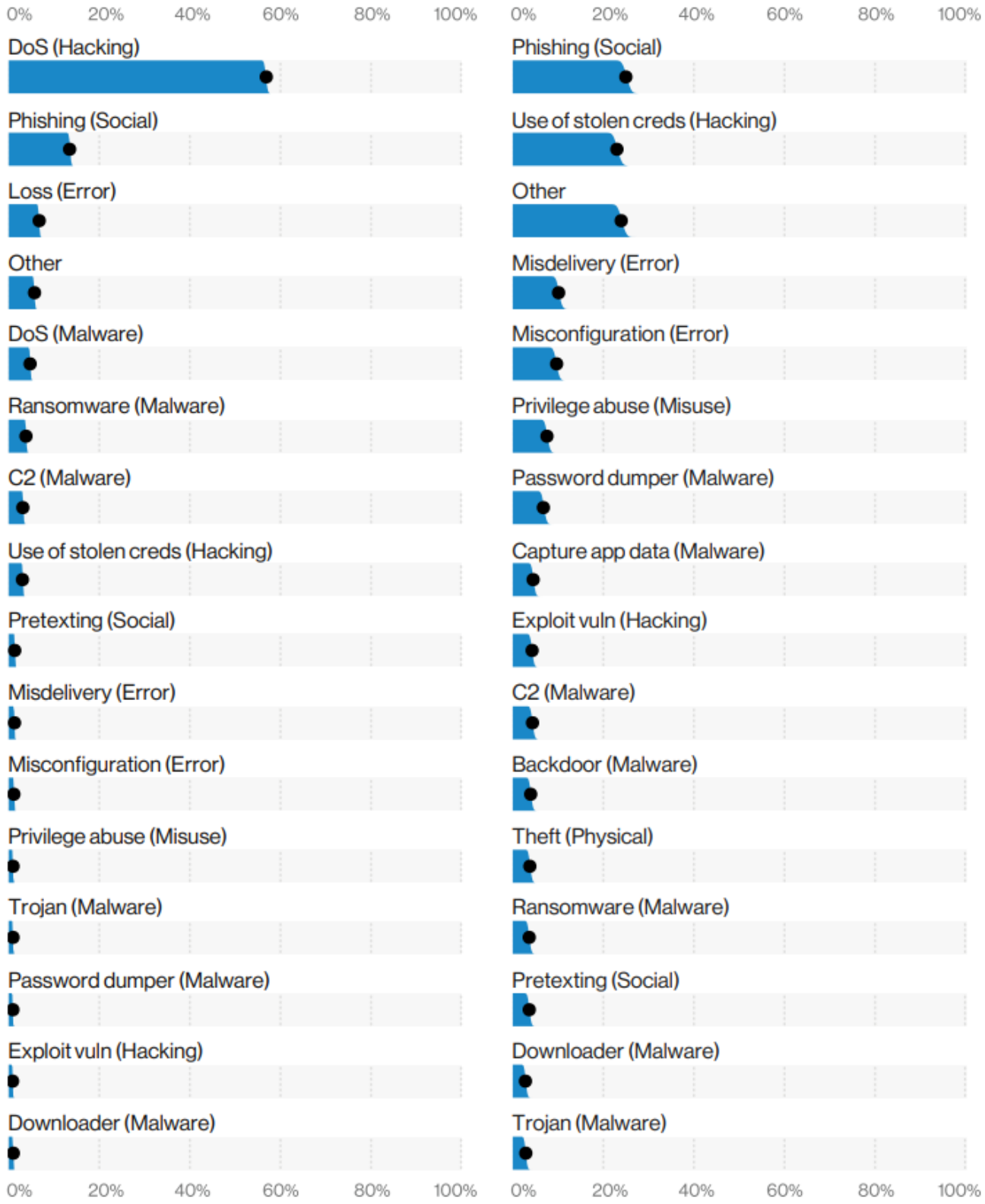

Рис. 1.1. Топ варіантів загрозливих дій в інцидентах (n = 23 619) та Топ варіантів загрозливих дій в порушеннях (n = 2,907) [1]

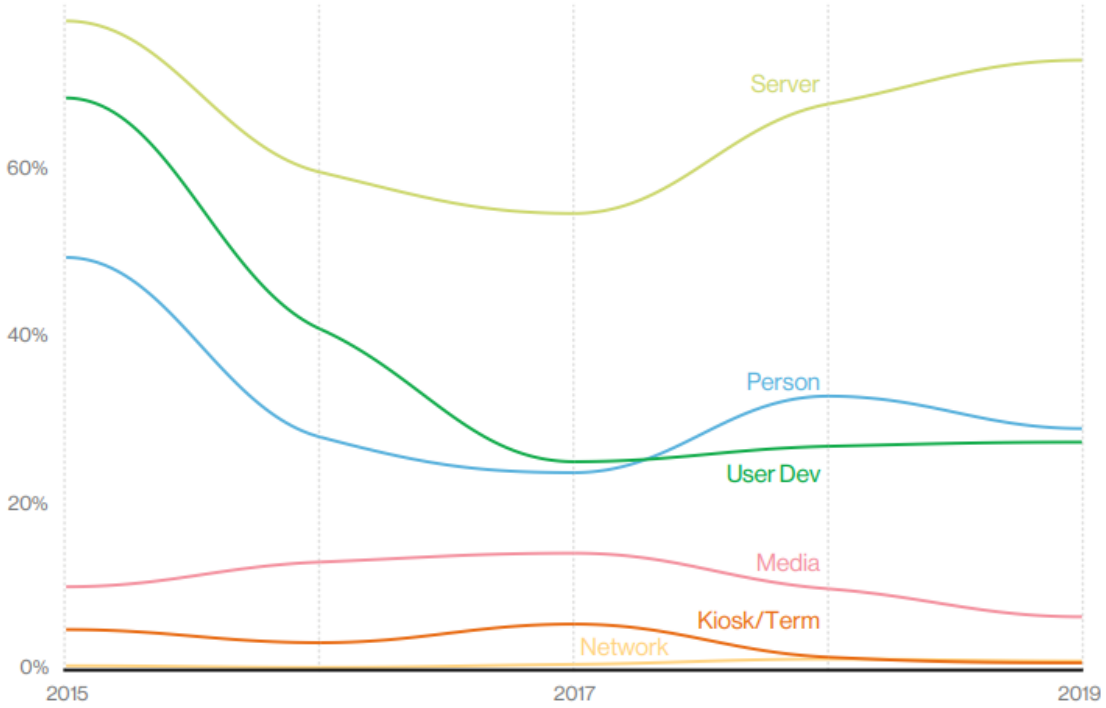

Рис. 1.2. Активи з плином часу в порушеннях [1]

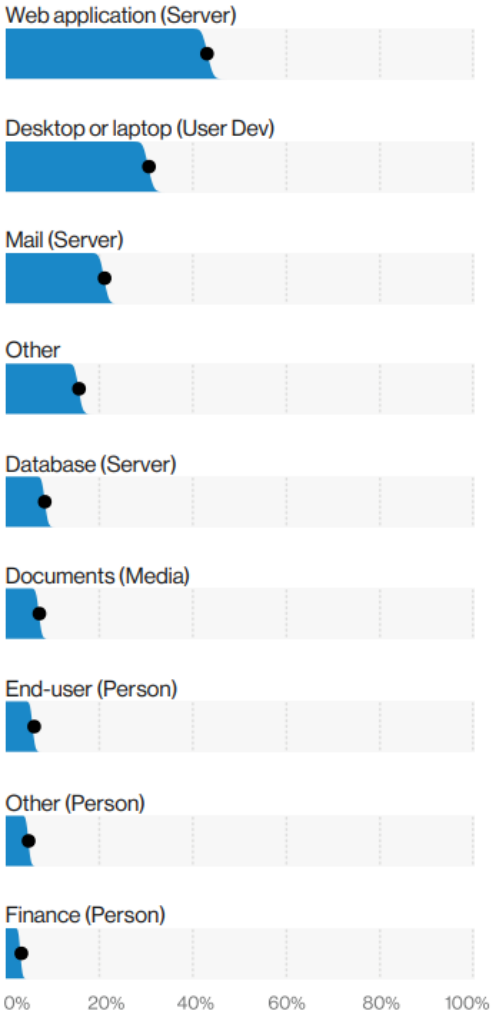

Рис. 1.3. Основні різновиди активів в порушеннях (n = 2,667) [1]

Компанії витрачають мільйони доларів щорічно на захист даних клієнтів, додатків, мереж і конфіденційної інформації. Проте, ці підприємства часто зламуються. Наприклад, 58% компаній зіткнулися зі значними інцидентами в сфері безпеки в минулому році, оскільки кількість загроз і витонченість атак у всьому світі зростає [2].

В результаті організації витрачають більше коштів на захист своїх мереж. У 2019 витрати на мережеву безпеку становили в середньому 9% бюджету витрат на технології безпеки, при цьому 54% осіб, які приймають рішення в області безпеки, очікували збільшення своїх витрат на мережеву безпеку в 2019 году [2].

У травні 2019 року VMware доручила Forrester Consulting розібратися в проблемах, з якими стикаються підприємства при захисті трафіку своєї внутрішньої мережі сервер-сервер. Компанія Forrester провела онлайн-опитування 224 фахівців з IT-безпеки, що відповідають за мережі, безпеку та інфраструктуру своїх організацій. Було виявлено, що, хоча існує багато технологій і послуг безпеки, реалізованих для захисту внутрішнього мережевого трафіку сервер-сервер, більшість компаній йдуть на неоптимальний компроміс між ступенем захисту і простотою операцій [2].

Організації по всьому світу усвідомлюють обмеження підходів до забезпечення безпеки на основі периметра і переходять до моделі з нульовою довірою. Фахівці з безпеки діють з помилковим відчуттям безпеки. Майже 59% фахівців з безпеки вважають, що вони ефективно захищають внутрішню мережу, проте, згідно з опитуванням Forrester Global Business Technographics Security Survey, 58% зіткнулися з серйозним інцидентом безпеки в минулому році [2].

Використання традиційних міжмережевих екранів периметра для захисту внутрішньої мережі неефективно. Сім з десяти підприємств страждають від надмірного використання міжмережевих екранів по периметру і вважають, що вони надмірно виділяють міжмережеві екрани, що може бути дорогим. П'ятдесят сім відсотків погодилися, що це означає компроміс між охопленням і операційної гнучкістю і маневреністю [2].

Обмежувальні політики міжмережевих екранів блокують гнучкість

розробників. Три чверті підприємств стикаються з проблемами, пов'язаними з швидкими темпами змін додатків, а 73% повідомляють, що ефективність надання політик міжмережевого екрану не встигає за темпами розробки.

Фахівцям з IT-безпеки потрібні вбудовані кросплатформні засоби управління безпекою, орієнтовані на додатки. Майбутнє безпеки залежить від заходів безпеки на основі додатків. Троє з п'яти респондентів вважають за краще вбудовані засоби управління безпекою рішенням на основі агентів [2].

Захист внутрішньої мережі за допомогою традиційних міжмережевих екранів не працює На підприємствах є багато продуктів і послуг для забезпечення безпеки, реалізованих для захисту периметра, внутрішньої мережі, хмарних сховищ, додатків і застарілої інфраструктури. Незважаючи на величезні інвестиції в рішення безпеки, ці компанії часто не використовують правильний інструмент для кожної середовища, що призводить до витрат, складності, відсутності прозорості та зниження безпеки [2].

Опитуючи професіоналів в області IT-безпеки, було виявлено чотири поширені проблеми з поточними середовищами безпеки [2]:

підприємства не забезпечують належний захист своїх внутрішніх мереж. Більше 75% компаній використовують віртуальні або фізичні міжмережеві екрани периметра для захисту внутрішнього мережевого трафіку. Однак 72% вважають, що їх надмірна залежність від міжмережевих екранів по периметру є серйозним викликом для безпеки їх внутрішньої мережі. Використання міжмережевих екранів периметра для захисту внутрішньої мережі вимагає закріплення трафіку і часто значної перебудови мережі, що вимагає компромісу між покриттям і простотою. Цей компроміс залишає прогалини в системі безпеки організації;

застарілі міжмережеві екрани – дорогий підхід до внутрішньої безпеки. Сім з десяти підприємств надмірно виділяють міжмережеві екрани – застаріла парадигма, яка вимагає великих витрат при використанні для трафіку зі сходу на захід. Крім того, 72% респондентів вважають, що відсутність адекватної сегментації мережі створює вразливості безпеки в організації. Забезпечення трафіку сервер-сервер відрізняється від захисту трафіку хост-сервер і вимагає

інших рішень;

непорівнянні рішення безпеки створюють проблеми інтеграції. Поширення пристроїв і безліч різних вимог і інструментів управління ставлять під загрозу стан безпеки. Понад три чверті компаній управляють десятьма або більше продуктами безпеки, і майже 20% управляють 50 або більше продуктами безпеки. *Не дивно, що більшість професіоналів в області IT-безпеки стикаються з серйозними проблемами інтеграції.* Відсутність інтеграції перешкоджає адаптованості, створює проломи в безпеці через неузгодження елементів управління і ускладнює управління;

фахівцям з IT-безпеки як і раніше не вистачає інформації про дії в мережі.

Підприємства не використовують розширені функції, оскільки менше однієї третини компаній повідомляють, що вони пишуть правила рівня 7 для фільтрації трафіку сервер-сервер. Незважаючи на кількість використовуваних продуктів, 73% фахівців з IT-безпеки вважають, що їм *не вистачає адекватних засобів контролю для моніторингу, фільтрації та аналізу трафіку сервер-сервер.* Майже три чверті вважають, що їм не вистачає інформації про дії в мережі. Забезпечення видимості всього центру обробки даних – це перший крок до надійної системи безпеки, чого не можуть забезпечити традиційні міжмережеві екрани периметра.

1.2. Призначення, принцип роботи та основні функції систем виявлення вторгнень

Виявлення вторгнень – це процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі, і їх аналізу на наявність ознак можливих інцидентів, які представляють собою порушення або неминучі загрози порушення політик комп'ютерної безпеки, політик допустимого використання або стандартних методів забезпечення безпеки [3].

Запобігання вторгненням – це процес виявлення вторгнень і спроби зупинити виявлені можливі інциденти. Системи виявлення й запобігання вторгненням (IDPS) в першу чергу орієнтовані на виявлення можливих інцидентів, реєстрацію інформації про них, спроби їх зупинити і повідомити про них адміністраторів

безпеки. Крім того, організації використовують IDPS для інших цілей, таких як виявлення проблем з політиками безпеки, документування існуючих загроз і утримання людей від порушення політик безпеки [3].

IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації. IDPS зазвичай записують інформацію, що відноситься до спостережуваних подій, повідомляють адміністраторів безпеки про важливі спостережувані події і створюють звіти. Багато IDPS також можуть реагувати на виявлену загрозу, намагаючись запобігти її успішному виконанню. Вони використовують кілька методів реагування, які включають в себе зупинку атаки IDPS, зміна середовища безпеки (наприклад, перенастроювання брандмауера) або зміна вмісту атаки [3].

Система виявлення вторгнень (IDS) – це програмне забезпечення, яке автоматизує процес виявлення вторгнень.

Система запобігання вторгнень (IPS) – це програмне забезпечення, яке має всі можливості системи виявлення вторгнень і може також намагатися зупинити можливі інциденти. Технології IDS і IPS пропонують багато можливостей і адміністратори зазвичай можуть відключати функції запобігання в продуктах IPS, змушуючи їх функціонувати як IDS.

Принципи виявлення і запобігання вторгнень

Інциденти мають безліч причин, наприклад шкідливі програми (черви, віруси), зловмисники, які отримують несанкціонований доступ до систем з Інтернету та авторизовані користувачі систем, які зловживають своїми привілеями або намагаються отримати додаткові привілеї, для яких вони не авторизовані. Хоча багато інцидентів носять зловмисний характер, багато інших – ні; наприклад, людина може неправильно ввести адресу комп'ютера і випадково спробувати без авторизації підключитися до іншої системи [3].

IDPS в першу чергу орієнтовані на виявлення можливих інцидентів. Наприклад, IDPS може виявити, коли зловмисник успішно скомпрометував систему, скориставшись уразливістю в системі. Потім IDPS може повідомити про інцидент адміністраторам безпеки, які можуть швидко ініціювати дії з реагування

на інцидент, щоб мінімізувати збиток, заподіяний інцидентом. IDPS може також реєструвати інформацію, яка може бути використана тими, хто розслідує інциденти [3].

IDPS також можна налаштувати для розпізнавання порушень політик безпеки. Наприклад, деякі IDPS можуть бути з настройками, аналогічними набору правил брандмауера, що дозволяє їм визначати мережевий трафік, який порушує політику безпеки або допустимого використання організації. Крім того, деякі IDPS можуть відслідковувати передачу файлів і виявляти підозрілі, наприклад копіювання великої бази даних на портативний комп'ютер користувача [3].

Багато IDPS також можуть ідентифікувати розвідувальну діяльність, яка може вказувати на неминучість атаки. Наприклад, деякі інструменти атак і шкідливі програми, зокрема черви, виконують розвідувальні операції, такі як сканування хостів і портів, для визначення цілей для подальших атак. IDPS може бути в змозі заблокувати розвідку і повідомити адміністраторів безпеки, які можуть вдатися до дій, якщо необхідно, змінити інші заходи безпеки для запобігання пов'язаних інцидентів. Оскільки в Інтернеті так часто ведеться розвідка, її виявлення часто виконується в першу чергу в захищених внутрішніх мережах [3].

Крім виявлення інцидентів і підтримки зусиль з реагування на інциденти, організації знайшли інші застосування для IDPS, включаючи наступне [3]:

виявлення проблем політики безпеки. IDPS може забезпечити певний рівень контролю якості для реалізації політики безпеки, наприклад, дублювання наборів правил брандмауера і попередження, коли він бачить мережевий трафік, який повинен був бути заблокований брандмауером, але не через помилки конфігурації брандмауера;

документування існуючої загрози для організації. IDPS реєструють інформацію про виявлені ними загрози. Розуміння частоти і характеристик атак на обчислювальні ресурси організації допомагає визначити відповідні заходи безпеки для захисту ресурсів. Інформацію також можна використовувати для інформування керівництва про загрози, з якими стикається організація;

стримування осіб від порушення політик безпеки. Якщо люди знають, що їх дії відстежуються технологіями IDPS на предмет порушень політики безпеки, вони з меншою ймовірністю здійснять такі порушення через ризик виявлення. Через зростаючої залежності від інформаційних систем, а також з-за поширеності і потенційного впливу вторгнень на ці системи IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації.

Ключові функції технологій IDPS

Існує багато типів технологій IDPS, які розрізняються в першу чергу типами подій, які вони можуть розпізнати, і методологіями, які вони використовують для ідентифікації інцидентів. Крім моніторингу та аналізу подій для виявлення небажаної активності, всі типи технологій IDPS зазвичай виконують такі функції [1]:

запис інформації, що відноситься до спостережуваних подій. Інформація зазвичай записується локально, а також може бути відправлена в окремі системи, такі як сервери централізованої реєстрації, рішення для управління інформацією і подіями (SIEM) і системи управління підприємством;

повідомлення адміністраторів безпеки про важливі спостережуваних події. Це повідомлення, відоме як попередження, відбувається за допомогою будь-якого з декількох методів, включаючи наступні: електронні листи, сторінки, повідомлення в призначеному для користувача інтерфейсі IDPS, пастки протоколу SNMP, повідомлення системного журналу, а також призначені для користувача програми і сценарії. Повідомлення зазвичай включає в себе тільки основну інформацію про подію, адміністраторам необхідно отримати доступ до IDPS для отримання додаткової інформації;

складання звітів. Звіти узагальнюють відслідковують події або надають детальну інформацію про конкретні події, що представляють інтерес. Деякі IDPS також можуть змінювати свій профіль безпеки при виявленні нової загрози. Наприклад, IDPS може збирати більш детальну інформацію для конкретного сеансу після виявлення шкідливої активності в цьому сеансі. IDPS може також змінити налаштування того, коли спрацьовують певні попередження або який пріоритет слід призначати наступним попередженням після виявлення конкретної

загрози.

Технології IPS відрізняються від технологій IDS однією характеристикою: технології IPS можуть реагувати на виявлену загрозу, намагаючись запобігти її успіх. Вони використовують кілька технік реагування, які можна розділити на наступні групи [3]:

IPS сама зупиняє атаку. Ось приклади того, як це можна зробити:

завершити підключення до мережі або призначений для користувача сеанс, який використовується для атаки;

заблокувати доступ до цілі (або, можливо, іншим імовірним цілям) з облікового запису порушника, IP-адреси або іншого атрибута зловмисника;

заблокувати будь-який доступ до цільового хосту, служби, додатку або іншого ресурсу.

IPS змінює середовище безпеки. IPS може змінити конфігурацію інших елементів управління безпекою, щоб запобігти атаці. Поширеними прикладами є перенастроювання мережевого пристрою (наприклад, брандмауера, маршрутизатора, комутатора) для блокування доступу зловмисника або цілі і зміна брандмауера на основі хоста на цілі для блокування вхідних атак. Деякі IPS можуть навіть викликати застосування виправлень до хосту, якщо IPS виявляє, що у хоста є вразливості [3].

IPS змінює зміст атаки. Деякі технології IPS можуть видаляти або замінювати шкідливі частини атаки, щоб зробити її безпечною. Простим прикладом є IPS, що видаляє заражене файлове вкладення з електронного листа, а потім роздільна очищеного електронного листа досягти його одержувача. Більш складним прикладом є IPS, який діє як проксі і нормалізує вхідні запити, що означає, що проксі переупаковують корисні дані запитів, відкидаючи інформацію заголовка. Це може привести до того, що деякі атаки будуть відкинуті як частина процесу нормалізації [3].

Ще одним поширеним атрибутом технологій IDPS є те, що вони не можуть забезпечити повністю точне виявлення. Коли IDPS неправильно ідентифікує доброякісну активність як шкідливу, відбувається помилкове спрацьовування.

Коли IDPS не може ідентифікувати шкідливу активність, відбувається помилково негативні результати. Неможливо усунути всі помилкові спрацьовування і негативи; в більшості випадків зменшення кількості входжень одного збільшує кількість входжень іншого. Багато організацій вважають за краще зменшувати кількість помилкових спрацьовувань за рахунок збільшення кількості помилкових спрацьовувань, що означає, що виявляється більше шкідливих подій, але потрібно більше ресурсів для аналізу, щоб відрізнити помилкові спрацьовування від справжніх шкідливих подій. Зміна конфігурації IDPS для підвищення точності виявлення називається настроюванням [3].

Більшість технологій IDPS також пропонують функції, які компенсують використання звичайних технік ухилення.

Ухилення – це зміна формату або часу зловмисної активності таким чином, щоб її зовнішній вигляд змінився, але ефект залишився колишнім. Зловмисники використовують методи ухилення, щоб не дати технологіям IDPS виявити їх атаки. Наприклад, зловмисник може кодувати текстові символи певним чином, знаючи, що мета розуміє кодування, і сподіваючись, що ніякі відстежують IDPS цього не роблять. Більшість технологій IDPS можуть подолати звичайні методи ухилення шляхом дублювання спеціальної обробки, виконуваної цілями. Якщо IDPS може «бачити» активність так само, як і ціль, тоді методи ухилення, як правило, не будуть успішними при приховуванні атак [3].

Існує багато типів технологій IDPS, які розрізняються в першу чергу типами подій, які вони можуть розпізнати, і методологіями, які вони використовують для виявлення можливих інцидентів.

Існуючі технологій IDPS [3]:

на основі мережі, яка відстежує мережевий трафік для певних сегментів мережі або пристроїв і аналізує активність протоколу мережі і додатків для виявлення підозрілої активності;

на основі безпроводового зв'язку, яка відстежує трафік безпроводової мережі і аналізує його для виявлення підозрілої активності, пов'язаної з самими протоколами безпроводової мережі;

аналіз мережевої поведінки (NBA), який досліджує мережевий трафік для виявлення загроз, які створюють незвичайні потоки трафіку, таких як DDoS-атаки, сканування і певні форми шкідливого ПЗ;

на основі хоста, який відстежує характеристики окремого хоста і події, що відбуваються всередині цього хоста, на предмет підозрілої активності.

Таблиця 1.1. Порівняння типів технологій IDPS [3]

IDPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor or Agent	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyze the widest range of application protocols; only IDPS that can thoroughly analyze many of them
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyze activity that was transferred in end-to-end encrypted communications

Більшість IDPS також пропонують функції, які компенсують використання звичайних методів ухилення, які змінюють формат або час шкідливої активності, щоб змінити її зовнішній вигляд, але не її ефект, щоб спробувати уникнути виявлення IDPS.

Більшість IDPS використовують кілька методологій виявлення, окремо або разом, щоб забезпечити більш широке і точне виявлення. Основні класи методів виявлення наступні [3]:

на основі сигнатури, який порівнює відомі сигнатури загроз з подіями, які спостерігаються, для виявлення інцидентів.

Це дуже ефективно при виявленні відомих загроз, але в значній мірі неефективно при виявленні невідомих загроз і багатьох варіантів відомих загроз. Виявлення на основі сигнатур не може відстежувати і розуміти стан складних комунікацій, тому воно не може виявити більшість атак, що складаються з декількох подій;

виявлення на основі аномалій, яке порівнює визначення того, яка діяльність вважається нормальною, з подіями, які спостерігаються, для виявлення значних відхилень. У цьому методі використовуються профілі, які створюються шляхом відстеження характеристик типової активності протягом певного періоду часу. Потім IDPS порівнює характеристики поточної активності з граничними значеннями, пов'язаними з профілем. Методи виявлення на основі аномалій можуть бути дуже ефективними при виявленні раніше невідомих загроз. Загальні проблеми з виявленням на основі аномалій включають ненавмисне включення зловмисних дій в профіль, створення профілів, які недостатньо складні для відображення реальної обчислювальної активності, і створення безлічі помилкових спрацьовувань;

аналіз протоколу з відстеженням стану, який порівнює заздалегідь певні профілі загальноприйнятих визначень доброякісної активності протоколу для кожного стану протоколу з подіями, які спостерігаються, для виявлення відхилень.

На відміну від виявлення на основі аномалій, яке використовує профілі, що залежать від хоста або мережі, аналіз протоколів з відстеженням стану спирається на розроблені постачальником універсальні профілі, які визначають, як конкретні протоколи повинні і не повинні використовуватися. Він здатний розуміти і відслідковувати стан протоколів, що дозволяє йому виявляти багато атак, які інші методи не можуть. Проблеми з аналізом протоколів з відстеженням стану включають в себе те, що часто дуже складно або неможливо розробити повністю точні моделі протоколів, це дуже ресурсномістких і не може виявляти атаки, які не порушують характеристики загальноприйнятої поведінки протоколу [3].

Перш ніж оцінювати продукти IDPS, організації повинні спочатку визначити загальні вимоги, яким вони повинні відповідати. Функції, що надаються продуктами IDPS, і які вживали методології значно різняться, тому продукт, який найкраще відповідає вимогам однієї організації, може не підходити для задоволення вимог іншої організації [3].

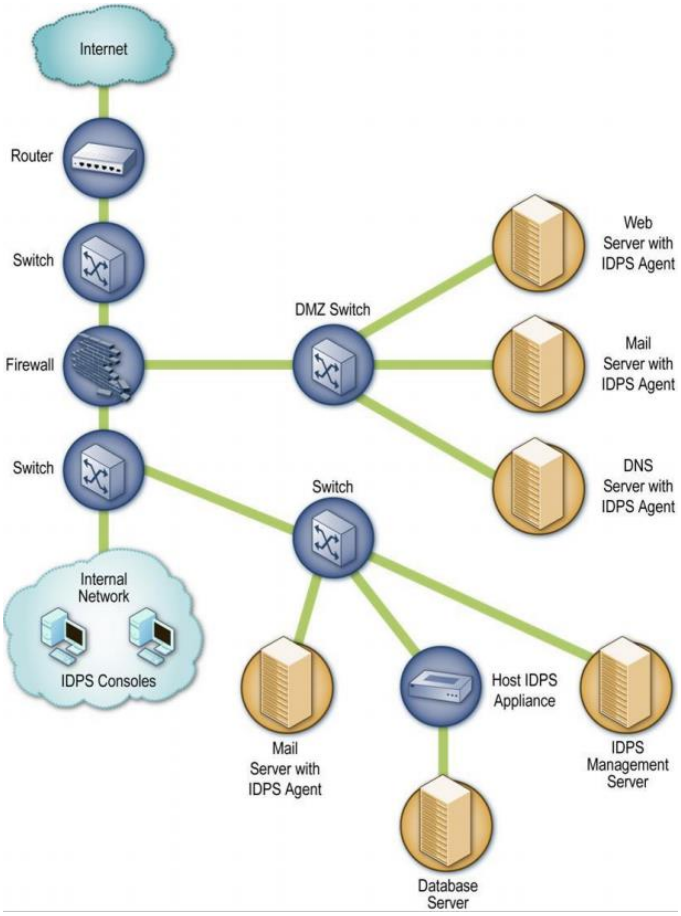

Рис. 1.4. Приклад архітектури розгортання агента IDPS на основі хосту [3]

Оцінювачам спочатку необхідно зрозуміти характеристики системного і мережевого середовищ організації і плани найближчих змін, щоб можна було вибрати IDPS, яка буде сумісна з ними і зможе відстежувати події в системах та/або мережах.

Ці знання також необхідні для розробки рішення IDPS. Отримавши розуміння існуючої системи і мережевого середовища, оцінювачі повинні сформулювати цілі і завдання, яких вони хочуть досягти за допомогою IDPS. Оцінювачі також повинні проаналізувати свої існуючі політики безпеки та інші IT-політики перед вибором продуктів. Політики служать специфікацією для багатьох функцій, які повинні забезпечувати продукти IDPS [3].

Крім того, оцінювачі повинні розуміти, чи підлягає організація нагляду або перевірки з боку іншої організації. Якщо так, вони повинні визначити, чи потрібні цього органу нагляду IDPS або інші ресурси безпеки конкретної системи. Оцінювачі також повинні враховувати обмеження ресурсів. Крім визначення

загальних вимог, оцінювачам також необхідно визначити більш спеціалізовані набори вимог [3]:

можливості безпеки, включаючи збір інформації, реєстрацію, виявлення і запобігання;

продуктивність, включаючи максимальну ємність і наведені цифри щодо;

управління, включаючи проектування і впровадження, експлуатацію та технічне обслуговування, а також навчання, документацію і технічну підтримку;

витрати на життєвий цикл, як початкові, так і експлуатаційні.

Організації можуть використовувати ці критерії в якості основи для створення специфічного для організації набору критеріїв, який враховує середовище, політику організації, а також існуючу безпеку і мережеву інфраструктуру. Після збору вимог і вибору критеріїв оцінювачам необхідно знайти надійні джерела інформації про продукти, які будуть оцінюватися. Загальні джерела даних про продукти включають в себе тестові лабораторії або випробування продуктів в реальних умовах, інформацію, надану постачальниками, сторонні огляди продуктів і попередній досвід IDPS, отриманий від окремих осіб в організації та довірених осіб в інших організаціях [3].

1.3. Аналіз існуючих методів та засобів виявлення та попередження вторгнень в інформаційну систему підприємства

Дослідницька компанія Forrester Consulting повідомляє, що 58% компаній зіткнулися зі значними інцидентами безпеки в 2019 році, незважаючи на те, що вони витратили більше коштів на захист своїх мереж [4].

Очевидно, що традиційних засобів захисту, таких як міжмережеві екрани по периметру, недостатньо для запобігання успішних атак. Фактично, згідно з опитуванням Forrester, проведеним на замовлення VMware, сім з десяти підприємств страждають від надмірного використання міжмережевих екранів по периметру [4].

Захист периметра не може зупинити зловмисника від бокового переміщення всередині корпоративної мережі для доступу до записів і їх ексфільтрації. У той же

час на атаки за участю інсайдерів, які вже знаходяться в периметрі, доводиться все більший відсоток зломів. Замість того, щоб покладатися на безпеку на основі периметра, організації повинні зосередитися на моніторингу, виявленні та блокування шкідливого внутрішнього трафіку в якості основного компонента своєї стратегії IT-безпеки.

У 2019 15,1 мільярда записів були виявлені в результаті більше 7000 публічно заявлених порушень, що зробило цей рік ще одним рекордним роком. Це являє собою збільшення кількості відкритих записів більш ніж на 284% в порівнянні з 2018 роком [4].

Згідно зі звітом Verizon про витоки даних за 2019 рік 69% порушень були здійснені сторонніми. Ці зовнішні кібератаки часто використовують таку тактику, як фішинг, для обходу міжмережевих екранів периметра і отримання доступу до внутрішньої мережі. Потім вони переміщаються в бік, щоб знайти і вилучити конфіденційні дані. Зовнішні кіберзлочинці також отримують вигоду від збільшеної площі атаки завдяки сьогоднішнім сучасним обчислювальним і прикладним середовищам [4].

Зазначається, що відсоток порушень, пов'язаних з внутрішніми суб'єктами, неухильно зростає з 2015 року. У 2019 приблизно 34% порушень, про які повідомляла Verizon, стосувалися внутрішніх суб'єктів. Ці внутрішні суб'єкти переміщуються через практично неконтрольований мережевий трафік в центрі обробки даних для досягнення своїх цілей [4].

Спостерігається зростаючий обсяг трафіку сервер-сервер. Засоби управління безпекою мережі, створені в епоху pre-DevOps, попередньо розподілених додатків, просто недостатні для захисту сьогоднішніх робочих навантажень і мікросервісів. Віртуальні машини (ВМ) підключаються до інших ВМ, контейнери підключаються до інших контейнерів, робочі навантаження підключаються до інших робочих навантажень і так далі. Все це створює великий обсяг мережевого трафіку всередині підприємства [4].

Щоб зрозуміти, чому зростаючий обсяг внутрішнього трафіку є важливим фактором безпеки, розглянемо поділ двох основних типів трафіку в мережі (див.

рис. 1.5):

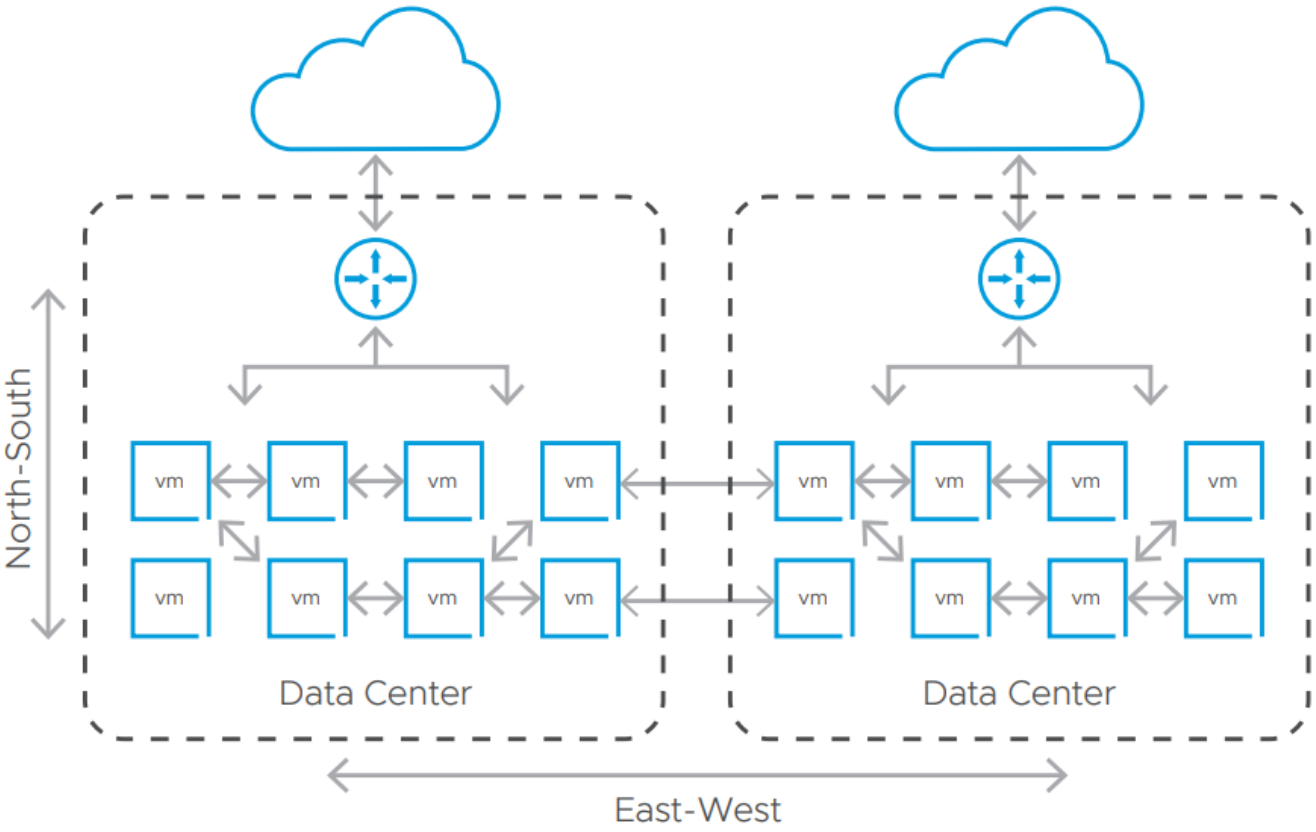

Рис. 1.5. Схема трафіку центру обробки даних [4]

Трафік хост-сервер, хост-хмара, сервер-хмара (північ-південь) є мережевим трафіком, що входить в мережу організації і виходить з неї. Трафік з півночі на південь зазвичай становить набагато менший відсоток від загального трафіку в мережі.

Внутрішній рафік (схід-захід) є трафіком, що переміщається горизонтально (отже, зі сходу на захід) через центр обробки даних, включаючи трафік від робочого навантаження до робочого навантаження (між центрами обробки даних, всередині центру обробки даних, з центру обробки даних в загальнодоступну хмару або з загальної хмари в центр обробки даних). У міру того як більш монолітні додатки замінюються розподіленими додатками або перебудовуються в них, обсяг трафіку зі сходу на захід (також відомого як внутрішній трафік) набагато перевищує обсяг трафіку з півночі на південь (вертикальний трафік, рис. 1.5) [4].

Брандмауер по периметру відстежує тільки трафік з півночі на південь. Проте, досвід, набутий з витоків даних за останнє десятиліття, полягає в тому, що організації не можуть припускати, що трафіку зі сходу на захід можна довіряти.

Довіра до всього трафіку зі сходу на захід означає, що кібератака, яка проходить через брандмауер периметра, може потім непоміченою переміщатися в межах мережі [4].

Для належного захисту від кіберзагроз, що проникають через периметр, а також від зловмисників зсередини, організаціям слід реалізувати *стратегію розподіленого внутрішнього брандмауера*. Внутрішні брандмауери проактивно забезпечують видимість і захист від внутрішніх загроз, а також мінімізують збиток від кібератак, що виходять за межі традиційного периметра мережі [4].

Правильний міжмережевий екран для правильного типу трафіку

В [4] зазначається, що у міру того як організації розуміють, що їм необхідно зосередити більше уваги, бюджету та зусиль на поліпшенні мережевої безпеки, вони багато роблять помилку, використовуючи традиційні міжмережеві екрани периметра, призначені для відстеження трафіку північ-південь для захисту своїх внутрішніх мереж. Хоча це може здатися привабливим, надання міжмережевих екранів периметра для моніторингу трафіку зі сходу на захід не тільки дорого, але і вкрай неефективно з точки зору забезпечення рівня контролю і продуктивності, необхідного для захисту великої кількості динамічних робочих навантажень [4].

Хоча периметр і внутрішні брандмауери забезпечують дотримання політик безпеки, відстежуючи і блокуючи потенційні загрози, характеристики трафіку схід-захід і топологія мережі означають, що підхід до забезпечення безпеки для брандмауера повинен бути іншим. Для брандмауера периметра допустимо блокувати трафік на основі портів, протоколів і IP-адрес або визначати трафік, що надходить або надходить від певної програми, такої як Skype [4].

З іншого боку, внутрішній брандмауер повинен працювати на більш детальному рівні, на рівні окремих робочих навантажень в додатку. На прикладі трирівневого додатку внутрішній брандмауер дозволяє трафік між веб-рівнем і рівнем прикладного додатку, а також між рівнем додатку і рівнем бази даних одного і того ж додатка. Однак він блокує трафік з веб-рівня на рівень бази даних, тому що цей трафік не повинен існувати в нормальному ході операцій [4].

Таким чином, ступінь деталізації примусу, необхідна для внутрішнього

брандмауера, набагато вище, ніж для брандмауера периметра. Типовий брандмауер периметра не знає, що (в прикладі з попереднього абзацу) три рівня належать одній і тій же додатком, але деякий трафік дозволений, в той час як інший трафік не знаходиться всередині цього додатка.

Масштаб і пропускна здатність

Централізований моніторинг трафіку з півночі на південь з використанням брандмауера по периметру зазвичай не створює вузьких місць для продуктивності, тому що обсяг трафіку не такий великий, як для трафіку зі сходу на захід. Однак у більшості підприємств трафік зі сходу на захід значно більше, ніж з півночі на південь. Якщо підприємство використовує брандмауер периметра для трафіку зі сходу на захід і хоче перевірити весь (або більшу частину) трафіку, йому доведеться розгорнути безліч брандмауерів периметра, щоб задовольнити свої вимоги до пропускної здатності.

Це може значно збільшити вартість і складність інфраструктури мережевої безпеки. Ось чому на практиці більшість організацій, що використовують брандмауери периметра для моніторингу трафіку зі сходу на захід, не перевіряють його більшу частину – витрати і обмеження для цього просто занадто великі. Для внутрішніх брандмауерів розподілений підхід до примусового застосування значно більш рентабельний, забезпечуючи необхідну масштабованість і продуктивність. Розподілений внутрішній брандмауер еластичний і підтримує автоматичне масштабування в міру збільшення або зменшення робочих навантажень. У міру збільшення кількості робочих навантажень ємність внутрішнього брандмауера збільшується автоматично. У міру того, як для підтримки розширення робочого навантаження використовується все більше серверів, невелика частина потужності сервера використовується для управління безпекою, що дозволяє відповідним чином масштабувати внутрішній брандмауер.

Вплив на інфраструктуру

Якщо рішення брандмауера периметра використовується для моніторингу трафіку зі сходу на захід, трафік примусово направляється до централізованого пристрою або можливостям і від них. Це створює візерунок у вигляді шпильки,

який в процесі використовує надмірну кількість мережевих ресурсів.

На додаток до збільшення затримки внутрішній мережевий трафік з працею ускладнює роботу як з точки зору дизайну мережі, так і з точки зору мережевих операцій. Мережі повинні бути спроектовані з урахуванням додаткового (непростого) трафіку, що проходить через міжмережевий екран периметра. З точки зору експлуатації, група операцій по забезпеченню безпеки повинна дотримуватися схеми мережі і враховувати обмеження при відправці додаткового трафіку для перевірки на міжмережевий екран [4].

В якості альтернативи, підхід з використанням розподіленого внутрішнього брандмауера дозволяє відстежувати великі об'єми трафіку зі сходу на захід без створення єдиної точки доступу. Розподілена архітектура переміщує примусове виконання ближче до даних, а не навпаки, і захищає весь трафік зі сходу на захід, зберігаючи при цьому низький вплив на мережеву та серверну інфраструктуру. Чи не відбувається закріплення трафіку, що усуває проблеми складності і затримки, пов'язані з використанням брандмауерів периметра для моніторингу внутрішньої мережі [4].

Видимість всередині програми

Моніторинг трафіку зі сходу на захід і застосування деталізованих політик вимагає прозорості аж до рівня робочого навантаження. Стандартні брандмауери периметра не дозволяють чітко бачити схеми взаємодії між робочими навантаженнями і мікросервісами, складовими сучасні розподілені додатки. Відсутність прозорості потоків додатків робить надзвичайно складним створення (і забезпечення дотримання) правил на рівні робочого навантаження або окремого потоку трафіку [4].

Для порівняння, внутрішній брандмауер повинен мати можливість автоматично визначати схему взаємодії між робочими навантаженнями і мікросервісами, давати рекомендації з політики безпеки на основі шаблону і перевіряти, чи відповідають потоки трафіку розгорнутим політикам. Надійний внутрішній брандмауер може виявляти і візуалізувати топологію додатків, процеси, допустимий стан, користувачів додатків і використовувані пристрої.

Управління життєвим циклом політики та мобільністю. Традиційні площині управління міжмережевими екранами призначені для роботи з десятками дискретних міжмережевих екранів, але не призначені для підтримки мобільності робочих навантажень з автоматичною перенастроюванням політик безпеки. Отже, коли брандмауер периметра використовується в якості внутрішнього брандмауера, оператори мережі та служби безпеки повинні вручну створювати нові політики безпеки щоразу, коли створюється нове робоче навантаження, і змінювати ці політики, коли робоче навантаження переміщається або виводиться з експлуатації [4].

Площина управління для внутрішніх міжмережевих екранів призначена для управління десятками тисяч об'єктів (включаючи віртуальні комутатори і розподілені міжмережеві екрани), при цьому забезпечуючи управління життєвим циклом політик і мобільність робочих навантажень. Внутрішній брандмауер автоматично налаштовує політики безпеки при створенні або зняття робочого навантаження без ручного втручання. Він підтримує мобільність робочих навантажень з відстеженням стану в рамках інфраструктури з безперешкодної пересиланням трафіку в нове місце і політиками безпеки, які автоматично переміщаються разом з віртуальною машиною робочого навантаження [4].

Необхідні компоненти внутрішнього брандмауера. Якщо традиційні міжмережеві екрани периметра не підходять або не ефективні в якості внутрішніх міжмережевих екранів, який тип рішення найкраще підходить для моніторингу трафіку схід-захід? Узагальнюючи вимоги з попереднього розділу, можна сказати, що внутрішній брандмауер повинен підтримувати [4]:

розподілене і детальне застосування політик безпеки;

масштабованість і пропускна здатність для обробки великих обсягів трафіку без зниження продуктивності;

незначний вплив на мережеву та серверну інфраструктуру;

видимість всередині програми;

мобільність робочих навантажень і автоматичне керування політиками.

Брандмауер по периметру не може задовольнити ці вимоги без виключно

високих витрат і складності, вимагаючи занадто великої кількості компромісів безпеки. Навпаки, розподілений програмно-визначений підхід є найбільш ефективним способом реалізації внутрішніх міжмережевих екранів для моніторингу горизонтального трафіку. Правильний програмно-визначений підхід до внутрішнього брандмауера забезпечує масштабованість, рентабельність і ефективність для захисту десятків тисяч окремих робочих навантажень в тисячах додатків [4].

Проте, не всі програмно визначені підходи можуть забезпечити рівень захисту внутрішньої мережі, необхідний підприємствам для захисту своїх чутливих робочих навантажень, без шкоди для детального контролю, узгодженості та гнучкості. Для досягнення оптимального покриття безпеки, продуктивності мережі і гнучкості експлуатації організаціям слід шукати спеціально створене рішення для внутрішнього брандмауера, що забезпечує внутрішню безпеку, вбудовану в інфраструктуру, розподілену і підтримуючу додатки [4].

Важливі варіанти використання внутрішніх брандмауерів. У міру того як все більше компаній усвідомлюють обмеження безпеки на основі периметра і ймовірність непомітного проходження шкідливого трафіку через внутрішню мережу, вони застосовують спеціальний програмно-визначений внутрішній брандмауер, щоб поліпшити свою загальну безпеку і захистити від кіберзагроз. Деякі з найбільш важливих варіантів використання стратегії внутрішнього брандмауера включають таке [4]:

віртуальні зони безпеки – внутрішні брандмауери можуть використовуватися для підтримки макросегментації бізнес-одиниць, партнерів, розробки з виробничих середовищ і інших вимог безпеки. Завдяки програмно визначеному підходу до внутрішніх міжмережевих екранів організації можуть створювати віртуальні зони безпеки і управляти ними без витрат і зусиль на покупку, настройку та обслуговування фізичних пристроїв;

виявлення бічного руху – перевірка всього руху зі сходу на захід дозволяє виявляти бічний рух на ранній стадії і обмежувати його пошкодження. Деталізовані політики на рівні робочого навантаження допомагають внутрішнім брандмауерам

блокувати спроби кіберзлочинців переміщатися в межах мережі для досягнення своїх цілей;

відповідність нормативним вимогам – для виконання вимог відповідності, таких як Закон про переносимість та підзвітність медичного страхування (HIPAA), Стандарт безпеки даних індустрії платіжних карт (PCI DSS) та Закон Сарбейнса-Окслі (SOX), розподілений внутрішній міжмережевий екран допомагає компаніям досягти відповідності. шляхом поширення політик безпеки, що залежать від правил, на всі відповідні робочі навантаження і відстеження потоків трафіку до конфіденційних додатків і від них. Програмні внутрішні брандмауери також позбавляють від необхідності купувати і розгортати окремі пристрої для забезпечення відповідності нормативним вимогам [4].

нульова довіра з використанням мікросегментації. Підхід з нульовим довірою передбачає, що всьому трафіку можна довіряти, поки політика не доведе зворотне. Мікросегментація – це основна концепція підходу з нульовим довірою, що дозволяє ізолювати робочі навантаження і захищати їх окремо. На підтримку підходу мікросегментації внутрішні брандмауери дозволяють організаціям логічно розділити центр обробки даних на окремі сегменти безпеки аж до індивідуального рівня робочого навантаження, а потім визначити елементи управління для кожного унікального сегмента [4];

консолідація засобів безпеки. Програмно визначені внутрішні брандмауери дозволяють організаціям позбутися від безлічі пристроїв безпеки і стримувати розростання пристроїв у міру того, як додатки стають більш розподіленими. Придбання меншої кількості пристроїв і керування ними знижує вартість володіння і спрощує операції по забезпеченню безпеки;

видимість. Групам операцій по мережі і безпеки необхідне розуміння і контекст всього трафіку робочих навантажень, щоб усунути сліпі плями безпеки і прискорити розслідування і усунення інцидентів. Правильний внутрішній брандмауер забезпечує повний огляд кожного робочого навантаження, використовує цю видимість для визначення очікуваної поведінки додатків і автоматично генерує політики безпеки для забезпечення свідомо правильної

поведінки [4].

Як висновок, щоб змінити темпи і обсяг витоку даних, підприємствам необхідно зосередити увагу на захисті всього свого горизонтального трафіку. Вони більше не можуть дозволити собі припустити, що захисту периметра буде досить і що трафіку в мережі можна довіряти. Програмно-визначене рішення, вбудоване в інфраструктуру, розподілене і підтримує додатки, є найбільш ефективним способом підвищення безпеки, зниження витрат і спрощення операцій. Єдине рішення, вбудоване в інфраструктуру, VMware Service-defined Firewall, призначене для захисту мережевого горизонтального трафіку в мультіхмарних середовищах. Зробивши безпеку невід'ємною частиною інфраструктури і віртуалізуючи весь стек безпеки, сервісно-визначений міжмережевий екран дозволяє групам безпеки знизити ризики, забезпечити відповідність вимогам і спростити операційну модель брандмауера для кожного робочого навантаження.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА НА БАЗІ РІШЕНЬ VMware NSX

2.1. Підхід виявлення та попередження вторгнень в інформаційну систему підприємства

Жодна організація чи підприємство не бажає порушення безпеки її даних та інформаційних систем. Тим не менше, кіберзлочинці порушують їх захист. Традиційних архітектур безпеки, очевидно, недостатньо, щоб відбити успішні атаки. Команди безпеки повинні припускати, що їх захист по периметру (включаючи їх брандмауери) буде врешті порушено. Їм потрібно серйозно задуматися над тим, щоб запобігти поперечному руху зловмисників усередині мереж організацій [6].

Колись мережевий периметр був чітко визначений і захищений, але став високо проникним через мобільних та віддалених кінцевих користувачів, персональні пристрої в мережах організацій та робочі навантаження (компоненти програм) у загальнодоступній хмарі. Навіть центр обробки даних, який колись розміщував лише спеціалізоване обладнання та додатки, тепер приймає кінцевих користувачів за допомогою технології інфраструктури віртуального робочого столу [6].

Після проникнення захист периметра не може перешкодити зовнішньому зловмисникові рухатися бічно всередині організаційної мережі, щоб дістати записи даних. Часто зловмисники зупиняються в мережі тижнями чи місяцями. Погіршуючи ситуацію, напади інсайдерів, які вже знаходяться в периметрі, становлять дедалі більший відсоток порушень. Інсайдери, можливо, навіть не бажають брати участь у порушенні – їхні облікові дані або пристрої кінцевого користувача можуть бути порушені зовнішнім зловмисником. Замість того, щоб покладатися виключно на безпеку периметра, організації повинні зосередитись на

виявленні та блокуванні шкідливого трафіку мережі «схід-захід» (внутрішній) як основний компонент стратегії безпеки інформаційних технологій (IT) [6].

Для цього потрібен внутрішній підхід брандмауера, спеціально розроблений для захисту великих обсягів трафіку центрів обробки даних схід-захід без шкоди для функціональності безпеки, продуктивності мережі або керованості. Такий підхід не тільки поліпшить стан безпеки організації, але й знизить загальну вартість володіння мережевими захисними структурами організації [6].

Розподілені внутрішні брандмауери запозичують розподілене застосування з рішень мікросегментації, щоб задовольнити вимоги до масштабу трафіку зі сходу на захід та деталізації. Одночасно вони зберігають здатність корпоративного брандмауера створювати та застосовувати політики безпеки на основі користувачів та додатків, а також включають контролери загроз, такі як IDS/IPS, NTA/NDR та пісочницю [6].

Тобто *розподілені внутрішні брандмауери* поєднують бажані можливості традиційних корпоративних брандмауерів та мікросегментаційні рішення для створення інноваційної архітектури брандмауера [6].

Як правило, наступним кроком до захисту центру обробки даних є початок переходу від макросегментації до мікросегментації, що дозволяє команді безпеки визначати та застосовувати більш детальні елементи управління. Команда безпеки вибирає добре зрозумілий та добре задокументований додаток, що важливо для бізнесу, який слід ізолювати.

Розглядаючи важливу програму для початку мікросегментації, організації часто починають з інфраструктури віртуального робочого столу (VDI). VDI, покращуючи керованість, витрати та захист даних для робочих столів користувачів, піддає інфраструктуру центру обробки даних загрозам, що виникають через порушення безпеки кінцевого користувача.

Однак, використовуючи службовий брандмауер, команда безпеки може ізолювати робочі столи від активів центру обробки даних, захистити інфраструктуру VDI та забезпечити керування доступом на основі користувачів, як показано на рис. 2.1.

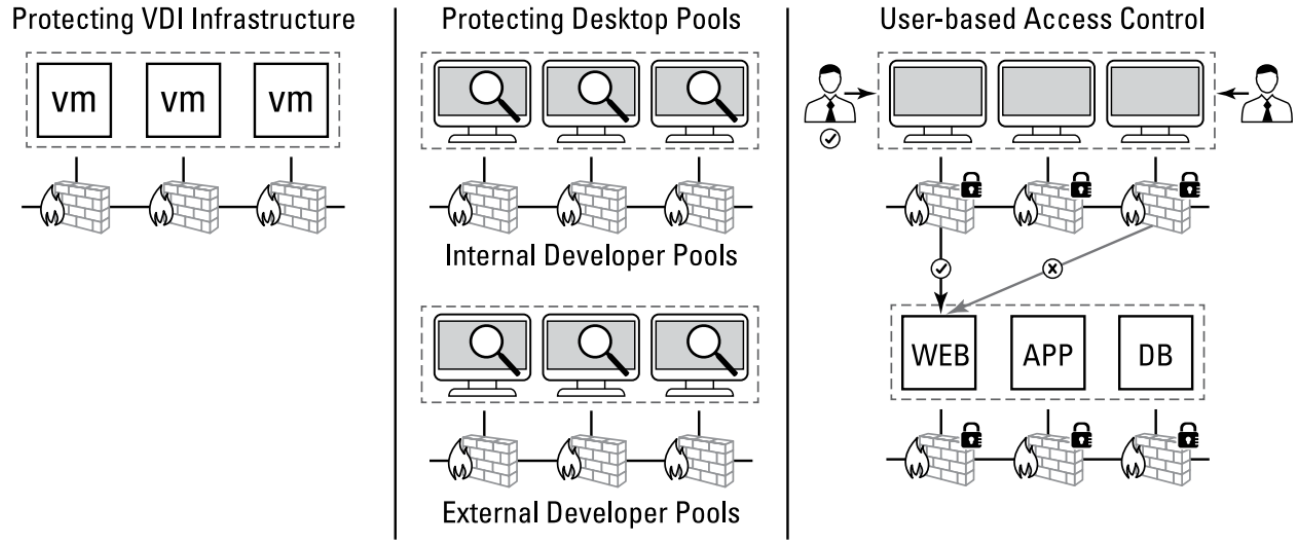

Рис. 2.1. Захищені середовища VDI [6]

Функція розподіленого виявлення/запобігання вторгненню (IDS/IPS) службового брандмауера дозволяє командам безпеки легко розгортати засоби управління загрозами для багаторівневого підходу до безпеки. Встановлення нового апаратного чи програмного забезпечення не потрібне. Оскільки службовий брандмауер вже розгорнуто, команда безпеки просто вмикає IDS/IPS [6].

Мікросегментація – це метод сегментації мережі на дрібномасштабному рівні, більш тонкому, ніж великомасштабна сегментація міжмережевих екранів на кордоні підприємства. Мікросегментація з'явилася в 2013 році, щоб задовольнити вимоги до масштабування трафіку і деталізації для захисту сучасних додатків. Однак рішення мікросегментації самі по собі створюють деякі проблеми. Більшість рішень мікросегментації не реалізують повний набір функцій безпеки, які забезпечуються міжмережевими екранами на кордоні підприємства [5].

Ці рішення є оркестратором, що використовують брандмауер, вбудований в операційні системи, на яких виконуються робочі навантаження. Оркестратор мікросегментації обмежений можливостями стандартних брандмауерів операційної системи. Зокрема, оркестратор не може розуміти або застосовувати політики на основі користувачів або додатків і не включають в себе будь-які механізми контролю загроз, такі як системи виявлення/запобігання вторгнень (IDS/IPS), аналіз мережевого трафіку/виявлення мережі та реагування (NTA/NDR) або пісочниця [5].

Розподілені внутрішні міжмережеві екрани запозичують розподілене застосування з рішень мікросегментації для задоволення вимог до масштабування і деталізації трафіку схід-захід. Одночасно вони зберігають здатність прикордонного брандмауера підприємства створювати і застосовувати політики безпеки на основі користувачів і додатків і включати засоби контролю загроз, такі як IDS/IPS, NTA/NDR і пісочниця. Тобто розподілені внутрішні міжмережеві екрани поєднують в собі бажані можливості традиційних міжмережевих екранів на кордоні підприємства і вирішення мікросегментації для створення інноваційної архітектури міжмережевих екранів.

Розподілені внутрішні брандмауери працюють не тільки з віртуалізованими центрами обробки даних, де робочі навантаження розміщуються на гіпервізора (програмному забезпеченні віртуалізації) на фізичному сервері. Вони також працюють з фізичними серверами (без гіпервізора), контейнерами і загальнодоступним хмарою аналогічно віртуалізувати серверів. Таким чином, розподілені внутрішні брандмауери можуть застосовувати єдиний набір політик для робочих навантажень незалежно від базової інфраструктури (локальне або загальнодоступне хмара) або типу робочого навантаження (віртуальна машина, фізичний сервер або контейнер) [5].

Для вирішення проблеми відсутності засобів контролю загроз групам безпеки часто необхідно розгортати засоби контролю загроз, такі як системи виявлення/запобігання вторгнень (IDS/IPS), щоб забезпечити другий рівень захисту в межах дозволеного трафіку. В одних випадках використання IDS/IPS пропонується державними або галузевими нормативними актами, а в інших цього вимагає внутрішня політика організації. Оскільки більшість операційних систем хоста не реалізують IDS/IPS, оркестратор мікросегментації не мають механізму для надання IDS/IPS в якості другого захисного рівня. В результаті групи безпеки отримують підтримку в придбанні і розгортанні спеціалізованого пристрою IDS/IPS або підтримки внутрішнього брандмауера з можливостями IDS/IPS (на додаток до оркестратора мікросегментації) [5].

IDS/IPS системи виявлення/запобігання вторгнень (IDS/IPS) – це програмне забезпечення або мережеве обладнання, розгорнуте для аналізу реального трафіку, що проходить через мережу. Розгортання IDS/IPS виявляють загрози, які прослизнули через контроль доступу, реалізований за допомогою брандмауера або рішення мікросегментації. Механізми регулярних виразів – це робочі конячки функціональності IDS/IPS. Ці механізми запрограмовані на пошук шаблонів трафіку, що вказують на загрози, з використанням мови конфігурації [5].

Групи безпеки називають шаблони, виражені за допомогою мови конфігурації IDS/IPS, сигнатурами. Крім того, більшість IDS/ IPS реалізують механізми декодування протоколу для перевірки відповідності між транзитним трафіком і опублікованими специфікаціями мережевого протоколу. Нарешті, деякі IDS/IPS виявляють аномальний трафік за допомогою статистичних методів. Такий трафік може вказувати на триваючі атаки [5].

Overlay-мережа – це логічна мережа, зазвичай побудована поверх фізичної мережі. Вона використовує базову фізичну мережу для транспортування трафіку, але інкапсулює пакети вихідних робочих навантажень всередині свого власного заголовка протоколу. Накладення мережі надає додаткові послуги, недоступні в фізичної мережі. Прикладом такої послуги є додавання сторонніх мережевих продуктів або продуктів безпеки в оверлейну мережу.

NSX і NSX Service-defined Firewall – це реалізації двох незалежних концепцій, і їх не слід плутати. NSX реалізує накладення мережі. Брандмауер NSX, який визначається службою, реалізує розподілений внутрішній брандмауер. Брандмауер, який визначається службою, працює однаково, незалежно від того, чи використовується накладення мережі або фізична мережа [5].

Досвідчені групи безпеки розуміють, що загрози часто поширюються всередині дозволеного трафіку. Наявність загроз всередині дозволеного трафіку є мотивацією для другого рівня захисту на додаток до контролю доступу. Системи виявлення й запобігання вторгнень (IDS/IPS) – популярна форма контролю загроз, широко використовувана в середніх і великих організаціях. Традиційні IDS/IPS,

автономні або як частина централізованого прикордонного брандмауера підприємства, знаходяться на шляху багатьох потоків трафіку [5].

Таким чином, вони повинні включати тисячі сигнатур виявлення загроз, щоб забезпечити охоплення всіх потоків трафіку. Кількість і тип включених сигнатур впливає на затримку і продуктивність IDS/IPS, а також на частоту помилкових спрацьовувань (помилкових попереджень). В результаті групи безпеки витрачають багато часу на налаштування своїх IDS/IPS.

Розподілений внутрішній брандмауер може включати в себе розподілений механізм IDS/IPS (або, в більш загальному сенсі, контроль загроз). Оскільки механізми розподілені, кожен механізм повинен запускати тільки сигнатури, застосовні до робочого навантаження, яку захищає механізм.

Таким чином, при робочому навантаженні включається лише невелика частина набору сигнатур, що знижує кількість помилкових спрацьовувань, які повинні обробляти групи безпеки.

Сервісно-визначений брандмауер VMware NSX – це спеціальний внутрішній брандмауер, повністю реалізований в програмному забезпеченні. Сервісно-визначений брандмауер включає наступні розподілені можливості [5]:

механізм контролю доступу (класичний міжмережевий екран з відстеженням стану, який також розпізнає додатки і користувачів/групи користувачів);

механізм аналітики;

механізм контролю загроз (IDS/IPS).

Системи контролю загроз, такі як IDS/IPS, NTA/NDR і пісочниці, потребують періодичного оновлення для підтримки їх ефективності. У разі IDS/IPS виявлення нових вразливостей призводить до випуску нових сигнатур. Ці оновлення сигнатур упаковуються в потік аналітики загроз з хмарної служби постачальника в системи IDS/IPS, розгорнуті замовником.

Для NTA/NDR і пісочниць аналітика загроз складається з IP-адрес і мережних доменів командно-керуючих серверів (використовуваних для управління діями шкідливих програм), точок розповсюдження шкідливих програм і шкідливих веб-сайтів. Аналітика загроз також включає характеристики і поведінку шкідливих

програм і шкідливих об'єктів, таких як файли. Стрічка інформації про загрози постачальника може включати в себе інші елементи, наприклад детальну інформацію про відомих вразливості в системах інформаційних технологій і звіти про атаки, які спостерігаються в клієнтській базі постачальника [5].

Функціональність розподіленого виявлення/запобігання вторгнень (IDS/IPS) в сервісно-визначеному міжмережевому екрані дозволяє службам безпеки легко розгортати засоби контролю загроз для багаторівневого підходу до безпеки. Установка нового обладнання або програмного забезпечення не вимагається. Оскільки брандмауер, який визначається службою, вже розгорнуто, група безпеки просто включає IDS/IPS.

Оскільки група безпеки використовує брандмауер, який визначається службою, в центрі обробки даних, він може зіткнутися з безліччю серверів і додатків, захищених автономними пристроями IDS/IPS. Часто використання IDS/IPS обумовлено вимогами організації або нормативними вимогами. З огляду на досвід, накопичений з IDS/IPS і захистом додатків в масштабі центру обробки даних на попередніх етапах, група безпеки вважатиме нескладним поетапне додавання IDS/IPS там, де це необхідно. При цьому група безпеки може вивести з експлуатації або перепрофілювати апаратні пристрої IDS/IPS.

2.2. Призначення та можливості рішення VMware NSX Distributed IDS/IPS щодо розширеного виявлення загроз

Рішення VMware NSX Distributed IDS/IPS надає адміністраторам безпеки програмне рішення IDS/IPS, яке дозволяє їм забезпечувати відповідність нормативним вимогам, створювати віртуальні зони і виявляти бічне переміщення загроз в трафіку хост-сервер [7].

Основними перевагами рішення VMware NSX [7] є:

гнучка пропускна здатність, яка полягає в усуненні вузьких місць в обладнанні за рахунок можливості перевірки, що автоматично масштабується з кожним робочим навантаженням;

спрощена мережева архітектура, яка сприяє уникненню необхідності

направляти трафік на централізовані пристрої і зменшенню перевантаження мережі за допомогою повністю розподіленої архітектури;

зменшення кількості помилкових спрацьовувань – більше робочих навантажень з нульовим кількістю помилкових спрацьовувань з ретельно підібраними наборами правил і більш точною відповідністю сигнатур на основі точного контексту програми;

підвищення ефективності використання ємності, сутність якого полягає у повторному використанні існуючих невикористаних обчислювальних ресурсів, усуваючи необхідність в додатково виділених пристроях.

В [7] зазначається, що сьогодні виникла зростаюча потреба в виявленні загроз трафіків сервер-сервер.

З появою розподілених додатків і мікросервісів внутрішній мережевий трафік тепер переважає над традиційним трафіком хост-сервер. У той же час межи центру обробки даних поширилися на периферійні і хмарні додатки, а також на пристрої кінцевих користувачів. Сучасні зловмисники помітили ці зміни і навчилися агресивно рухатися убік, починаючи з початкової точки атаки. В результаті перевірка внутрішнього трафіку сервер-сервер за допомогою розширених можливостей виявлення загроз стає все більш критичною для захисту робочих навантажень і корпоративних даних [7].

Розподілена IDS/IPS ламає традиційні компроміси безпеки. VMware Service-defined Firewall являє собою єдиний спеціалізований внутрішній міжмережевий екран, який захищає трафік сервер-сервер. Він віртуалізує і розподіляє весь стек безпеки для кожного робочого навантаження і надає багатий набір можливостей міжмережевого екрану, включаючи елементи управління доступом рівня 4 і елементи управління мережею рівня 7 з відстеженням стану [7].

Можливості сервісно-визначеного міжмережевого екрану тепер включають систему виявлення вторгнень і систему запобігання вторгнень (IDS/IPS). IDS/IPS вже давно є стандартними можливостями стека мережевої безпеки. Однак вартість і операційна складність обмежили їх використання певними сегментами мережі, на

периметрі підприємства до загальнодоступних мереж або на кордонах зон відповідності нормативним вимогам [7].

VMware NSX Distributed IDS/IPS пропонує принципово нову архітектуру (рис. 2.2), яка порушує цей традиційний компроміс між широтою охоплення безпеки і складністю експлуатації. Він використовує повністю програмний розподілений підхід, який переносить перевірку трафіку на кожне робоче навантаження і усуває необхідність направляти трафік на окремі пристрої. Оперативна простота розгортання і управління функціями IDS/IPS при кожному робочому навантаженні забезпечує повне покриття без будь-яких білих плям [7].

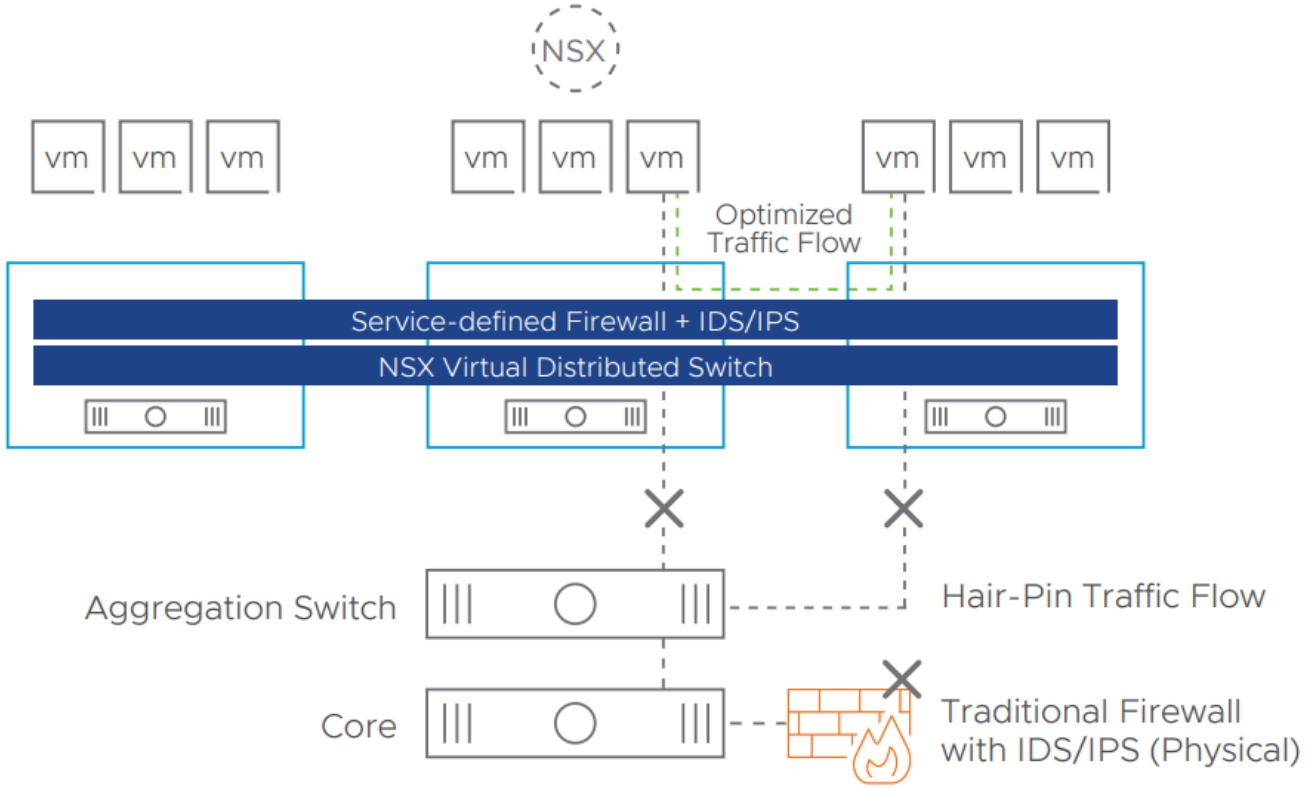

Рис. 2.2. Компоненти архітектури VMware NSX Distributed IDS/IPS [7]

VMware NSX Distributed IDS/IPS – це програма для управління трафіком, призначена для аналізу внутрішнього трафіку сервер-сервер та виявлення бічних рухів загроз. Механізм працює в межах гіпервізора для оптимізації перевірки пакетів. VMware NSX Distributed IDS/IPS поєднує провідні в галузі набори сигнатур, декодери протоколів та механізми, що базуються на виявленні аномалій, для пошуку відомих та невідомих атак у потоці трафіку. Він також отримує

переваги від розширеного контексту додатка, знижуючи помилкові позитивні показники, одночасно вимагаючи мінімальних обчислювальних витрат на хості [7].

Застосування рішення VMware NSX Distributed IDS/IPS дозволяє [7]:

легко досягти відповідності нормативним вимогам – застосування перевірки трафіків для делікатних програм, розгорнувши програмне забезпечення, не купуючи дорогих приладів;

віртуалізація зони безпеки – створення і налаштування кількох віртуальних зон безпеки для внутрішніх команд та партнерів, не вимагаючи фізичного відокремлення мережі;

заміна дискретних (апаратних) приладів – використання можливостей IDS/IPS, властиві NSX, замінюючи традиційні прилади IDS/IPS, зменшуючи вартість та складність;

виявлення поперечного руху загроз – перевірка трафіків сервер-сервер при кожному навантаженні, використовуючи методи сигнатурау, виявлення на основі аномалій та перевірку відповідності протоколу.

Основні можливості рішення VMware NSX Distributed IDS/IPS [7]:

Розподілений аналіз. Механізм IDS/IPS розподіляється по кожному робочому навантаженню, усуваючи сліпі зони, зберігаючи просту операційну модель. Потужність перевірки масштабується лінійно залежно від кількості робочих навантажень, усуваючи обмеження пропускної здатності, як правило, при застосуванні дискретних приладів.

Куратор, розподіл сигнатураів на основі контексту. Рівень управління дозволяє оцінювати лише відповідні сигнатураи загроз при кожному навантаженні на основі знань про запущені програми. Це зменшує обчислювальні накладні витрати на хости і призводить до вищих збігів вірності з нижчими коефіцієнтами помилково позитивних.

Виявлення загроз, керованих контекстом програми. Механізм IDS/IPS має остаточні знання про програми, що працюють на кожному хості, усуваючи здогадки щодо контексту вихідного або цільового додатків. Ці знання дозволяють

покращити класифікацію попереджень та можливість оператора визначати пріоритети попереджень для подальшого розслідування.

Політика та мобільність налаштувань. Коли робочі навантаження рухаються, політики та налаштування змінюються разом із навантаженням. Робочі навантаження автоматично захищаються в новому місці без ручної конфігурації або втрати потоків.

Автоматизоване управління життєвим циклом політики. Модель політики NSX дозволяє автоматично створювати політики безпеки для нових робочих навантажень та руйнувати старі політики, коли робочі навантаження виводяться з експлуатації. Політика безпеки залишається узгодженою із розгорнутими робочими навантаженнями, запобігаючи накопиченню застарілих політик, що є загальним викликом для традиційних пристроїв мережевої безпеки.

Таким чином, рішення VMware NSX Distributed IDS/IPS розширює підхід до внутрішньої безпеки, додавши нові можливості виявлення загроз. Воно охоплює основні принципи програмно-визначеного міжмережевого екрану – вбудовувати безпеку в інфраструктуру та розподіляти її на всі робочі навантаження, роблячи безпеку повсюдною та простою.

Рішення VMware NSX Distributed IDS/IPS досліджує унікальний контекст додатків від гіпервізора та рівнів віртуалізації мережі, щоб зробити виявлення загроз більш точним, ефективним та динамічним [7].

2.3. Принципи роботи рішення VMware NSX Distributed IDS/IPS

Системи виявлення вторгнень (IDS) з'явилися в кінці 1990-х для виявлення схем потоків трафіку, що свідчать про проведені атаки. У 2000-х рішення IDS трансформувалися в системи запобігання вторгнень (IPS), оскільки придбали додаткові можливості забезпечення безпеки. З роками система IDS/IPS стала стандартним компонентом стека мережі і безпеки [8].

Незважаючи на це, через вартість і експлуатаційну складність область застосування IDS/IPS обмежувалася окремими сегментами мережі, наприклад, які знаходяться на периметрі організацій з загальнодоступними мережами. У міру

розвитку розподілених додатків і мікросервісів мережевий трафік в ЦОД також виріс в рази. У той же час межі ЦОД стали розмитими через зростаючі можливості підключення додатків в ЦОД до публічної хмари і пристроїв кінцевих користувачів. В результаті організації стали набагато частіше використовувати IDS/IPS як рівня безпеки ЦОД [8].

Вбудована система безпеки в VMware NSX – основа стратегії безпеки VMware. Це вбудована в інфраструктуру система, розподілена по IT-середовищу і яка враховує вимоги додатків. Брандмауер VMware SDF, вбудований в платформу VMware NSX рівнів 2–7, є результатом реалізації цієї стратегії в ЦОД. Він дозволяє адміністраторам одночасно забезпечувати безпеку горизонтального трафіку в усіх багатохмарних середовищах [8].

Платформа NSX призначена для двох основних сценаріїв використання в ЦОД: віртуалізація мережі і забезпечення безпеки горизонтального трафіку. Віртуалізація мережі відокремлює управління потоками трафіку від базової фізичної мережі. Захист горизонтального трафіку дозволяє задавати і застосовувати політики безпеки в ЦОД з деталізацією на рівні потоків трафіку за допомогою засобів безпеки, розташованих в гіпервізорі. Комплексна віртуалізація мережі і системи безпеки забезпечує високу гнучкість архітектури мережі ЦОД і в той же час надає *вбудовану систему безпеки* [8].

За рахунок своєї архітектури NSX вбудовує систему безпеки в інфраструктуру віртуалізації мережі. Засоби безпеки завжди присутні в інфраструктурі, тому їх не потрібно розгортати окремо. Більш того, можливість несанкціонованого доступу до засобів управління безпекою виключена, оскільки вони розташовані в гіпервізорі, що відокремлює їх від цільової області атаки (тобто робочого навантаження) [8].

NSX має розподілену архітектуру. Засоби управління безпекою розташовані у віртуальному мережевому інтерфейсі кожного робочого навантаження і надають гнучкий механізм для контролю потоків трафіку. При цьому відсутній централізований пристрій, що обмежує ресурси системи безпеки, тому немає

необхідності в штучній прив'язці мережевого трафіку до стека засобів мережевої безпеки [8].

Нарешті, оскільки платформа NSX інтегрована в інфраструктуру віртуалізації, вона забезпечує візуалізацію всіх додатків і робочих навантажень. NSX використовує цю візуалізацію для визначення широкого контексту додатків, докладного відстеження життєвого циклу робочих навантажень і автоматизації управління політиками безпеки.

Функції VMware NSX Distributed IDS/IPS забезпечують додаткові можливості перевірки трафіку для брандмауера SDF. Для IDS/IPS застосовуються ті ж принципи вбудованої системи безпеки, що і для брандмауера SDF. Тому переваги брандмауера SDF поширюються і на NSX Distributed IDS/IPS [8].

Роботу IDS/IPS забезпечують модулі регулярних виразів, що визначають схеми потоків трафіку. Ці модулі запрограмовані на пошук відомих загроз на основі схем потоків трафіку за допомогою мови конфігурації. Оператори мережі і систем безпеки використовують схеми, виражені за допомогою мови конфігурації IDS/IPS, як сигнатур. В даний час в більшості систем IDS/IPS крім виявлення загроз на основі сигнатур використовуються такі методи забезпечення безпеки, як перевірки відповідності протоколів і портів, а також виявлення аномального трафіку [8].

Системи IDS/IPS регулярно підключаються до приватних хмар для оновлення інформації про виявлення, в тому числі про сигнатури. Цю інформацію, передану в режимі реального часу, створюють, тестують і поширюють організації з дослідження загроз, які відстежують нові типи вразливостей [8].

Системи IDS/IPS можна впроваджувати у вигляді автономних спеціалізованих пристроїв або в складі брандмауера. У першому випадку системи IDS/IPS працюють в прихованому режимі на другому рівні стека протоколу. У другому випадку система аналізує трафік, попередньо дозволений в брандмауері, і функціонує на третьому рівні стека протоколу [8].

Більшість традиційних систем IDS/IPS на сучасному ринку (як автономних, так і інтегрованих з брандмауером) – це окремі централізовані пристрої. Оператори

встановлюють ці пристрої на невеликій кількості попередньо обраних ділянок мережі, на яких необхідна перевірка трафіку за допомогою систем IDS/IPS.

Системи NSX Distributed IDS/IPS були створені в рамках Suricata, відомого і широко визнаного проекту з відкритим вихідним кодом. Платформа NSX розширює можливості Suricata, надаючи модулям IDS/IPS середовище виконання, включаючи функції контролю мережевих операцій введення-виведення і управління [8].

NSX поєднує функції IDS/IPS і брандмауера, що забезпечує однопрохідну структуру аналізу трафіку. Спочатку весь трафік проходить через брандмауер, а потім виконується аналіз IDS/IPS в залежності від конфігурації. Крім того, поєднання функцій IDS/IPS і брандмауера спрощує визначення і застосування політик мережевої безпеки [8].

Як показано на рис. 2.3, системи NSX Distributed IDS/IPS розміщені в області користувача і підключені до модуля брандмауера, який знаходиться в ядрі гіпервізора. Один додаток взаємодіє з іншим, відправляючи трафік в гіпервізор, в якому брандмауер аналізує його. Далі брандмауер направляє трафік в модуль IDS/IPS в області користувача [8].

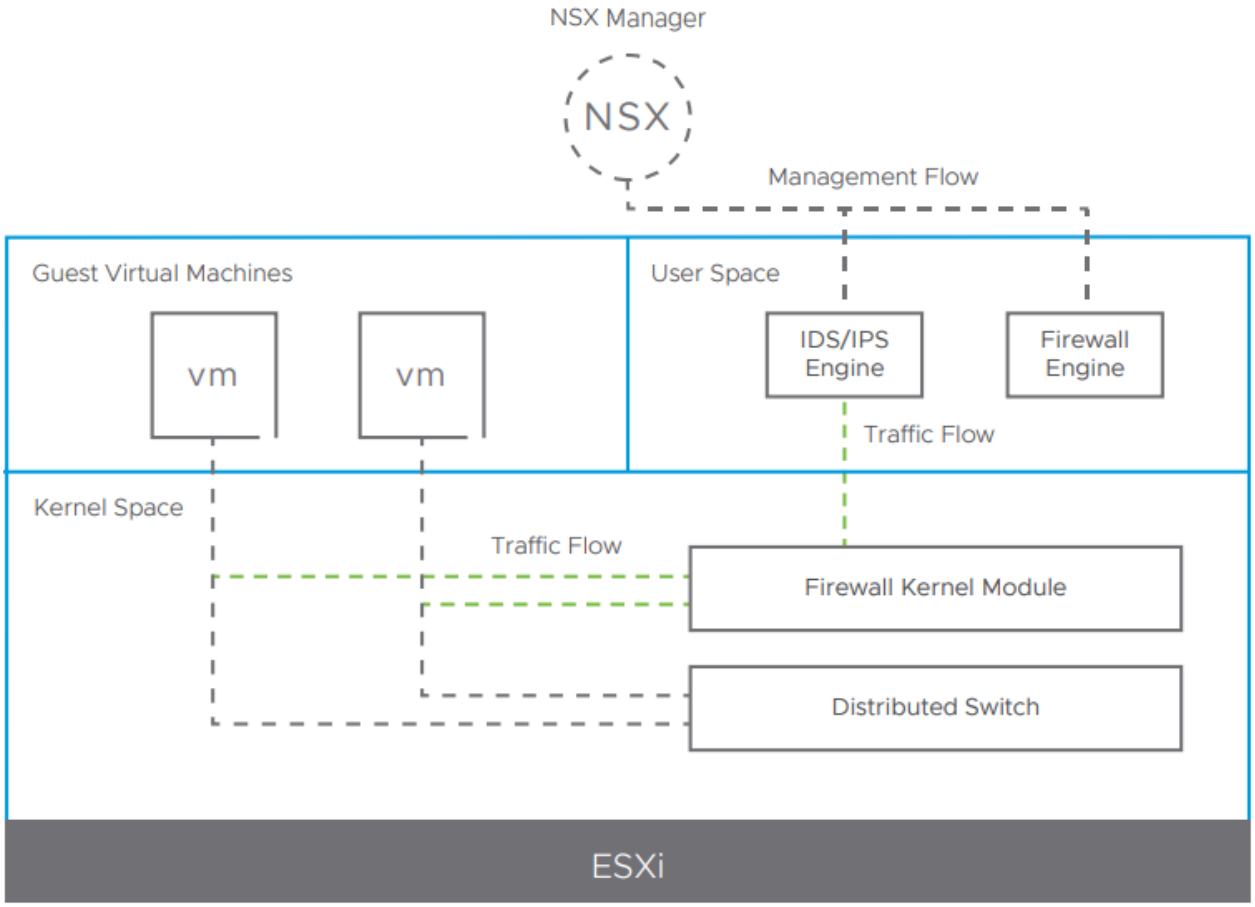

Рис. 2.3. Брандмауер и IDS/IPS в NSX [8]

Модуль IDS/IPS використовує сигнатури, декодери протоколів і виявлення аномалій для пошуку атак в потоці трафіку. Якщо атак не виявлено, трафик направляється назад в брандмауер для подальшої відправки в місце призначення. Якщо ж атака виявлена, створюється і записується оповіщення [8].

Процес аналізу IDS/IPS на вузлі призначення, який отримує трафік, аналогічний вищеописаному. Однак оператори можуть відмовитися від аналізу IDS/IPS в середовищі призначення (або в джерелі), якщо вважає, що аналізу IDS/IPS на одному кінці потоку трафіку досить [8].

Переваги NSX Distributed IDS/IPS

Архітектура NSX Distributed IDS/IPS кардинально відрізняється від архітектури традиційних систем IDS/IPS. Різниця пов'язана з тим, що в традиційних системах IDS/IPS аналіз виконується централізовано на окремому віртуальному або фізичному пристрої. Система NSX, навпаки, розподілена і повністю інтегрована з інфраструктурою віртуалізації [8].

Оптимізований потік трафіку. Оператори розгортають IDS/IPS разом з брандмауером або за ним в точці входу / виходу трафіку ЦОД. Потоки трафіку в ЦОД, що вимагають аналізу IDS/IPS, направляються до централізованого пристрою і повертаються від нього, створюючи схему перенаправлення і витрачаючи при цьому мережеві ресурси. NSX усуває перенаправлення і спрощує структуру мережі завдяки розміщенню модуля IDS/IPS разом з джерелом або місцем призначення потоку трафіку, як показано на рис. 2.

Ніяких обмежень при аналізі. У традиційних систем IDS/IPS на пристрої IDS/IPS або в брандмауері ресурси для аналізу обмежені. Щоб додавати додаткові ресурси, операторам доводиться постійно оновлювати апаратні пристрої до новітнього покоління, а це дорого і пов'язано з перериваннями роботи. NSX Distributed IDS/IPS використовує вільні ресурси на серверах, де працюють захищені додатки, і лінійно масштабується в міру додавання нових робочих навантажень. Таким чином, ресурси для аналізу не обмежені, що дозволяє використовувати великий обсяг ресурсів для аналізу трафіку ЦОД [8].

Повне покриття для всього трафіку. З огляду на описані вище обмеження, оператори мережі та системи безпеки змушені вибирати трафік для аналізу IDS/IPS. Часто системи IDS/IPS забезпечують аналіз тільки незначній частині трафіку, що надходить в брандмауер. В інших випадках автономні системи IDS/IPS розміщуються глибоко всередині мережі та забезпечують захист незначної кількості серверів, що ускладнює мережеву структуру. Система NSX є розподіленою, завдяки чому модулі IDS/IPS можна використовувати для аналізу всіх потоків трафіку для всіх робочих навантажень, що усуває «сліпі зони». У операторів є можливості точного налаштування функцій IDS/IPS для кожного робочого навантаження без обмежень, пов'язаних з базовими структурами мережі [8].

Контроль та налаштування сигнатур на основі контексту. Оскільки традиційні системи IDS/IPS централізовані і через них проходить безліч потоків трафіку, їм необхідно включати тисячі сигнатур, щоб забезпечити покриття всіх потоків трафіку. При великій кількості включених сигнатур і різноманітності їх

типів виникають затримки в роботі систем IDS/IPS і знижується їхня пропускна здатність. В результаті оператори витрачають багато часу на налаштування сигнатур IDS/IPS. Рішення NSX Distributed IDS/IPS враховує потреби додатків і дає можливість адаптувати сигнатури для кожного робочого навантаження. Щоб зменшити ймовірність помилкових спрацьовувань, для робочого навантаження можна включити тільки невелику кількість сигнатур [8].

Крім того, модуль IDS/IPS може змінювати рівень серйозності сповіщень, що створюються при виявленні відповідних сигнатур, залежно контексту програми і важливості робочого навантаження, яке захищається. Наприклад, сповіщення в базі даних кредитних карт може вимагати більшої уваги в порівнянні з іншими робочими навантаженнями [8].

Підтримка мобільності робочих навантажень. Віртуалізація ЦОД дозволяє переносити робочі навантаження в інший вузол або ЦОД (за допомогою vMotion). При використанні традиційних систем IDS/IPS неможливо зручно і швидко перенастроювати політики безпеки з урахуванням нового місця розташування робочого навантаження. У NSX політики безпеки переміщаються разом з віртуальною машиною (ВМ) робочого навантаження. В результаті трафік залишається повністю захищеним, незалежно від того, куди була переміщена ВМ. Крім того, під час переміщення не відбуваються втрати трафіку або розриви підключення, оскільки NSX відразу ж перенаправляє трафік в нове місце розташування [8].

Автоматизоване управління життєвим циклом політик. Традиційні системи IDS/IPS не враховують життєвий цикл програм, безпеку яких забезпечують. Через це операторам мережі і систем безпеки доводиться вручну задавати нові політики безпеки при створенні нових робочих навантажень і змінювати їх при виведенні робочих навантажень з експлуатації. Часто оператори побоюються допустити помилки при частому створенні нових політик або видаленні застарілих, що ускладнює підтримку актуальності систем безпеки. Завдяки динамічним групам в NSX оператори можуть підтримувати актуальність політик без ризику внесення помилок. NSX автоматично налаштовує політики безпеки при створенні або

виведенні з експлуатації робочого навантаження, запобігаючи появі незахищених робочих навантажень і накопичення застарілих політик безпеки [8].

Сценарії використання NSX Distributed IDS/IPS

Завдяки поєднанню функцій IDS/IPS з брандмауером SDF платформа NSX дозволяє операторам вирішувати додаткові проблеми з безпекою [8].

Забезпечення відповідності із законодавством. У множині ЦОД розміщуються додатки, що містять конфіденційну інформацію, наприклад медичні або фінансові дані. Часто такі додатки повинні відповідати нормативним вимогам стандартів HIPAA в сфері охорони здоров'я і PCI DSS або SOX в сфері фінансів. Нормативні вимоги регулюють використання IDS/IPS для запобігання витоку або крадіжки даних [8].

За допомогою рішення Distributed IDS/IPS, яке входить до складу NSX, оператори мережі та систем безпеки можуть забезпечити відповідність вимогам, вибірково задіючи системи IDS/IPS тільки для робочих навантажень додатків, що містять конфіденційні дані. Завдяки програмному підходу NSX виконує складну частину роботи, застосовуючи політики безпеки для всіх відповідних робочих навантажень. Це усуває необхідність купувати і розгортати окремі пристрої або брандмауери. Для більш детального аналізу і моніторингу відповідності нормативним вимогам оператори можуть відслідковувати вхідні та вихідні потоки трафіку в важливих додатках за допомогою таких засобів, як VMware NSX Intelligence [8].

Впровадження віртуальних зон. Деяким організаціям потрібно встановити прямі мережеві підключення до організацій-партнерів. Інші організації розглядають бізнес-підрозділи і дочірні компанії як орендарів центрального IT-відділу. Оператори мережі і систем безпеки можуть забезпечити відповідність зазначеним вище вимогам за допомогою NSX, використовуючи брандмауер і IDS/IPS для впровадження віртуальної зони. Оператори можуть додавати нових партнерів і орендарів без необхідності замовляти, встановлювати і налаштовувати нові апаратні брандмауери або системи IDS/IPS. Аналогічним чином оператори

можуть відключати партнерів і орендарів, не залишаючи незадіяним обладнання, придбане раніше [8].

Заміна окремих пристроїв IDS/IPS. Оператори мережі і систем безпеки час від часу змінюють архітектуру частин ЦОД для консолідації функцій безпеки. Оператори, які вже прийняли рішення віртуалізувати мережі ЦОД, тепер можуть замінити окремі централізовані пристрої IDS/IPS розподіленої платформою NSX. Це дає операторам мережі і систем безпеки можливість управляти функціями брандмауера і системи IDS/IPS з єдиної консолі управління (VMware NSX Manager) [8].

Виявлення горизонтального поширення загроз. Зловмисники, яким вдається проникнути в ЦОД, зазвичай намагаються здійснити горизонтальний перехід від ВМ, в які вони проникли, до інших ВМ, на яких розміщені конфіденційні дані. Щоб виконати таке горизонтальне переміщення, зловмисники проводять розвідку за допомогою таких засобів, як Netcat. Системи IDS/IPS з відповідними сигнатурами можуть виявити спроби розвідки і оповістити про них операторів мережі та систем безпеки. Далі оператори можуть блокувати дії зловмисників (в тому числі за допомогою IDS/IPS) або відслідковувати їх, використовуючи NSX Intelligence або інші засоби [8].

NSX Intelligence і NSX Distributed IDS/IPS

NSX Intelligence – це розподілена система збору даних та аналізу безпеки, доступ до якої можна отримати за допомогою NSX Manager (консолі управління NSX).

NSX Intelligence ефективно збирає метадані з гіпервізора в середовищі NSX і зберігає інформацію для подальшого використання. NSX Intelligence створює деталізовані схеми залежностей додатків, які забезпечують візуалізацію робочих навантажень і потоків в мережі, допомагаючи операторам отримати загальний огляд середовища. Крім того, NSX Intelligence автоматично рекомендує політики безпеки брандмауера на основі виявлених схем потоків трафіку між додатками, що значно спрощує впровадження мікросегментації і внутрішнього брандмауера. Нарешті, NSX Intelligence безперервно відстежує кожен потік трафіку і дозволяє

операторам застосовувати політики безпеки до потоків, щоб продемонструвати і підтримувати відповідність нормативним вимогам щодо безпечності [8].

NSX Intelligence органічно доповнює брандмауер SDF і систему IDS/IPS як рівня візуалізації та керування політиками. NSX Intelligence, брандмауер SDF і система IDS/IPS разом утворюють комплексний і зручний в розгортанні стек внутрішнього брандмауера, що забезпечує реалізацію стратегії вбудованої системи безпеки в ЦОД.

3 ПОРЯДОК ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА

3.1. Порядок втілення та застосування системи виявлення та попередження вторгнень в інформаційну систему підприємства

Сервісно-визначений міжмережевий екран VMware є рішення для захисту горизонтального трафіку в мультіхмарних середовищах і складається з трьох основних компонентів (рис. 3.1). Перш за все, у нас є розподілений міжмережевий екран, який дозволяє виконувати мікросегментацію. Розподілений брандмауер, по суті, є брандмауером в ядрі, який знаходиться на vNIC (віртуальний контролер мережевого інтерфейсу) кожного робочого навантаження в середовищі, забезпечуючи будь-який рівень фільтрації, мікросегментацію між рівнями додатка або макросегментацію, наприклад, ізолюючи виробництво від робочих навантажень розробки, або щось середнє між ними, повністю незалежне від основної мережі. VMware перетворили розподілений міжмережевий екран в повноцінний міжмережевий екран рівня 7 з відстеженням стану [9].

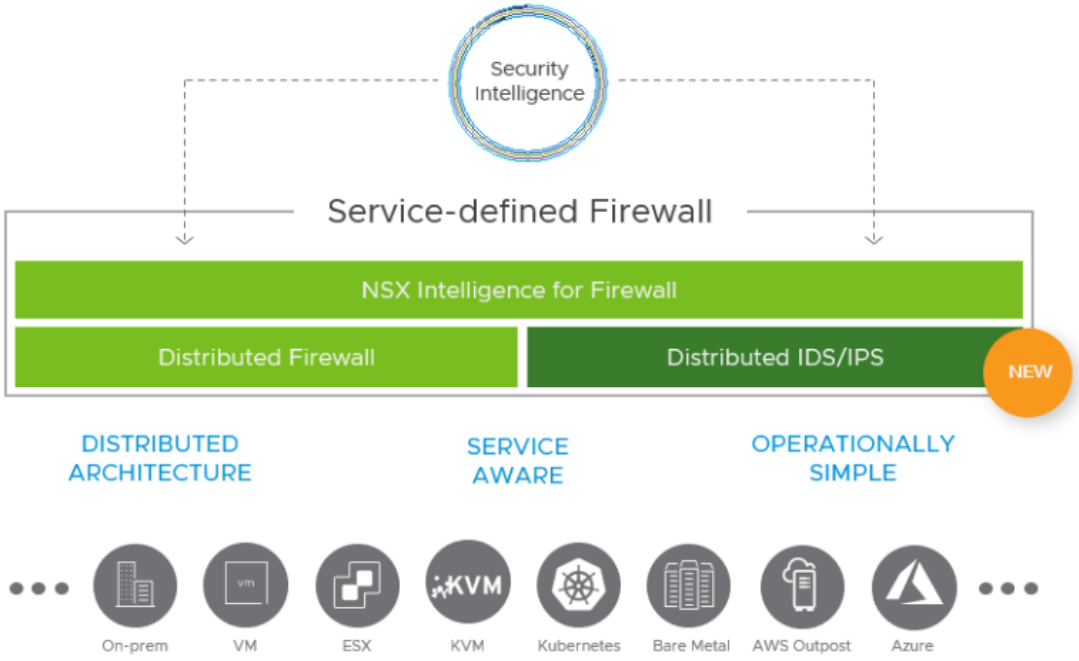

Рис. 3.1. VMware Service-defined Firewall [9]

NSX Intelligence є розподіленою платформою візуалізації і аналітики, повністю інтегрованою в NSX, яка забезпечує видимість всіх потоків *без необхідності покладатися на традиційні механізми, такі як Netflow або копіювання всього трафіку*, а також забезпечує формулювання політики, яка дозволяє клієнтам отримати повну мікросегментацію. IDS/IPS, яка заснована на розподіленій архітектурі та дозволяє клієнтам мати мережеву IDS/IPS, яка знаходиться на vNIC кожного робочого навантаження зі здатністю перехоплювати кожен потік без необхідності закріплювати будь-якої трафік незалежно від підключення до мережі [9].

Одна з ключових проблем традиційних мережевих рішень IDS/IPS полягає в тому, що вони покладаються на величезний обсяг трафіку, який повинен бути закріплений або скопійований на централізований пристрій IPS. Це часто пов'язано з мережевою архітектурою, а також означає, що зростаючі організації повинні постійно додавати брандмауери або пристрої IDS в свій централізований кластер, щоб не відставати від зростаючого обсягу трафіку, який вимагає перевірки [9].

Ще одна проблема, пов'язана з цими рішеннями, полягає в тому, що вони не забезпечують захист від бокового поширення атак в межах певного сегмента мережі. Якщо у нас є дві робочі навантаження додатків, розгорнуті тут в одній і тій же VLAN, немає ніякого реального способу вставити вбудований пристрій IPS між цими робочими навантаженнями і повторити це для всіх робочих навантажень у всьому центрі обробки даних [9].

Крім того, в віртуалізованих центрах обробки даних, завдяки використанню DRS і vMotion, робочі навантаження часто переміщаються на інші хости, кластери або центри обробки даних. Це означає, що трафік тепер перенаправляється на інший пристрій IPS, який не має контексту існуючого потоку і може навіть мати іншу політику.

Нарешті, централізовані мережеві IDS/IPS дуже погано розуміють контекст потоку. Вони просто дивляться на мережевий трафік, нічого не знаючи про те, звідки цей потік і чи є об'єкт атаки потенційно вразливим. В результаті весь трафік повинен відповідати кільком тисячам сигнатур. Сигнатури, які виявляють експлойт

проти вразливості в Apache, також застосовуються до сервера, на якому працює MySQL, і так далі [9].

Це призводить до двох ключових проблем: одним з них є велика кількість помилкових спрацьовувань, через які адміністратору безпеки складно відрізнити важливі події, що вимагають негайних дій, від всіх інших, особливо якщо події не включають контекст про те, хто є жертвою і що відбувається з цією машиною. Друга проблема, пов'язана з пропуском всього трафіку через всі сигнатури, полягає в тому, що це значно знижує пропускну здатність.

Розподілена IDS/IPS NSX поєднує в собі деякі з кращих якостей IPS-рішень на основі хоста з кращими якостями IPS-рішень для мережевих баз, щоб надати радикально інше рішення, яке дозволяє виявляти і запобігати вторгнення на рівні деталізації робочого навантаження і в масштабі всієї системи [9].

Подібно операційної моделі розподіленого брандмауера, розподілена IDS/IPS NSX розгортається в гіпервізорі при наявності NSX-T. Це не вимагає розгортання будь-яких додаткових пристроїв на цьому гіпервізорі, на гостьовій віртуальної машині або де-небудь в мережі. Замість того, щоб направляти трафік до централізованого пристрою IDS по мережі, IDS застосовується прямо в джерелі або пункті призначення потоку, коли він покидає робоче навантаження або входить. Як і у випадку з розподіленим міжмережевим екраном, існує необхідність необхідно змінити архітектуру мережі для застосування IDS/IPS для перевірки трафіку між робочими навантаженнями незалежно від того, чи є ці робочі навантаження одним і тим же VLAN, логічним сегментом або іншим VLAN [9].

Розподілений міжмережевий екран і IDS/IPS застосовуються до трафіку ще до того, як він потрапить на розподілений комутатор. Практично завжди фактична мета атаки відрізняється від того, де зловмисник спочатку отримав доступ. Це означає, що зловмисник спробує пройти через середовище, щоб вкрасти цінні дані, які йому потрібні. Отже, здатність захищатися не тільки від початкового вектора атаки, але і від бокового зміщення є критичною. Мікросегментація з використанням розподіленого брандмауера є ключем до зменшення поверхні атаки і значно ускладнює горизонтальне переміщення, і тепер вперше стає оперативно

здійсненним інтерфейс кожної з робочих навантажень за допомогою служби виявлення і запобігання вторгнень. Необхідно блокувати спроби використання вразливостей, де б вони не існували, і незалежно від того, чи намагається зловмисник отримати початковий доступ в середовищі або вже скомпрометував робоче навантаження в тій же VLAN і тепер намагається перейти до своєї цільової базі даних в тій же VLAN [9].

Найбільші і найбільш успішні клієнти в значній мірі покладаються на контекст при мікросегментації їх середовища. Вони використовують групи безпеки, засновані на тегах і інших конструкціях, для створення політики, яка прив'язана безпосередньо з самим додатком, а не з мережевими конструкціями такими, як IP-адреси і порти. Цей же контекст також є дуже важливою відмінністю, яка вирішує дві ключові проблеми, характерні для традиційних рішень IDS і IPS [9].

Завдяки тому, що дане рішення вбудоване в гіпервізор, є можливість доступу до набагато більшої кількості контексту, ніж ми могли б просто дізнатися, сидячи в мережі. Якщо ми знаємо, наприклад, назву кожного робочого навантаження, додаток, частиною якого він є, тощо інструменти VMware і Guest Introspection framework можуть надати нам додатковий контекст, такий як версія операційної системи, яка працює на кожному гостьовому комп'ютері, і навіть те, який процес або користувач створив конкретний потік. Якщо відомо, що сервер бази даних вразливий для конкретної вразливості, яка використовується прямо зараз, очевидно, що це вимагає негайної уваги, в той час як мережевий адміністратор, який запускає сигнатуру IPS, виконуючи сканування, повинен бути набагато менш серйозною проблемою [9].

Крім включення відповідної пріоритезації, той же контекст також можна використовувати для зменшення кількості помилкових спрацьовувань і збільшення кількості робочих навантажень з нульовим позитивним результатом, оскільки у нас є гарне уявлення про те, чи є ціль потенційно вразливою. Таким чином, зменшується кількість попереджень, які часто дуже великі при використанні традиційних мережевих рішень [9].

Нарешті, використовуючи контекст, можна включити тільки сигнатури, що відносяться до робочих навантажень, що захищається. Якщо розподілений екземпляр IDS застосовується до сервера Apache, можна включити тільки релевантні сигнатури, а не переважну більшість сигнатур, що не відносяться до цього робочого навантаження. Це різко знижує вплив на продуктивність, що спостерігається при використанні традиційних IDS/IPS [9].

IDS/IPS NSX надає розподілену, повсюдну площину примусового застосування. Однак розподілена модель IPS NSX дає додаткові переваги. NSX IPS – це IPS, розподілена по всім хостам [10].

Як і у випадку з DFW (Distributed Firewall), розподілений характер IPS дозволяє лінійно збільшувати пропускну здатність разом з обчислювальною потужністю. Однак, крім цього, поширення IPS дає додаткову перевагу. Це доданий контекст [10].

Успадковані мережеві системи виявлення та запобігання вторгнень розгортаються централізовано в мережі і покладаються або на проходження трафіку через них, або на копію трафіку, що відправляється їм за допомогою таких методів, як SPAN або TAP [10].

Ці датчики зазвичай зіставляють весь трафік з усіма або широким набором сигнатур і мають дуже мало інформації про активи, які вони захищають. Застосування всіх сигнатур до всього трафіку дуже неефективно, тому що IDS/IPS, на відміну від брандмауера, повинен дивитися на корисне навантаження пакета, а не тільки на мережеві заголовки. Кожна сигнатура, яку необхідно зіставити з трафіком, додає накладні витрати на перевірку і потенційну затримку [10]. Крім того, оскільки застарілі мережеві пристрої IDS/IPS просто бачать пакети, не маючи контексту про захищених робочих навантаженнях, групам безпеки дуже складно визначити відповідний пріоритет для кожного інциденту. Очевидно, що успішне вторгнення на вразливий сервер бази даних у виробничому середовищі, на якому зберігаються критично важливі дані, вимагає більшої уваги, ніж будь-хто з IT-персоналу, який запускає подію IDS шляхом сканування вразливостей [10].

Оскільки розподілена IDS/IPS NSX застосовується до vNIC кожної робочої навантаження, немає необхідності прив'язати трафік до централізованого пристрою, і можна дуже вибірково вибирати, які сигнатури застосовуються. Сигнатури, пов'язані з уразливістю Windows, не потрібно застосовувати до робочих навантажень Linux, або серверам під управлінням Apache не потрібні сигнатури, які виявляють експлойт служби бази даних. Через гостьову платформу самоаналізу і гостьові драйвери NSX має доступ до контексту кожного гостя, включаючи версію операційної системи, користувачів, які увійшли в систему, або будь-який запущений процес. Цей контекст можна використовувати для вибіркового застосування тільки відповідних сигнатур, не тільки зменшуючи вплив на обробку, але, що більш важливо, зменшуючи шум і кількість помилкових спрацьовувань в порівнянні з тим, що можна було б побачити, якби всі сигнатури застосовувалися до всього трафіку з допомогою традиційного устрою [10].

Як і у випадку з NSX DFW, NSX IPS не залежить від мережі і може використовуватися для контролю вторгнень як робочих навантажень на традиційні VLAN, так і робочих навантажень на overlay-сегментах.

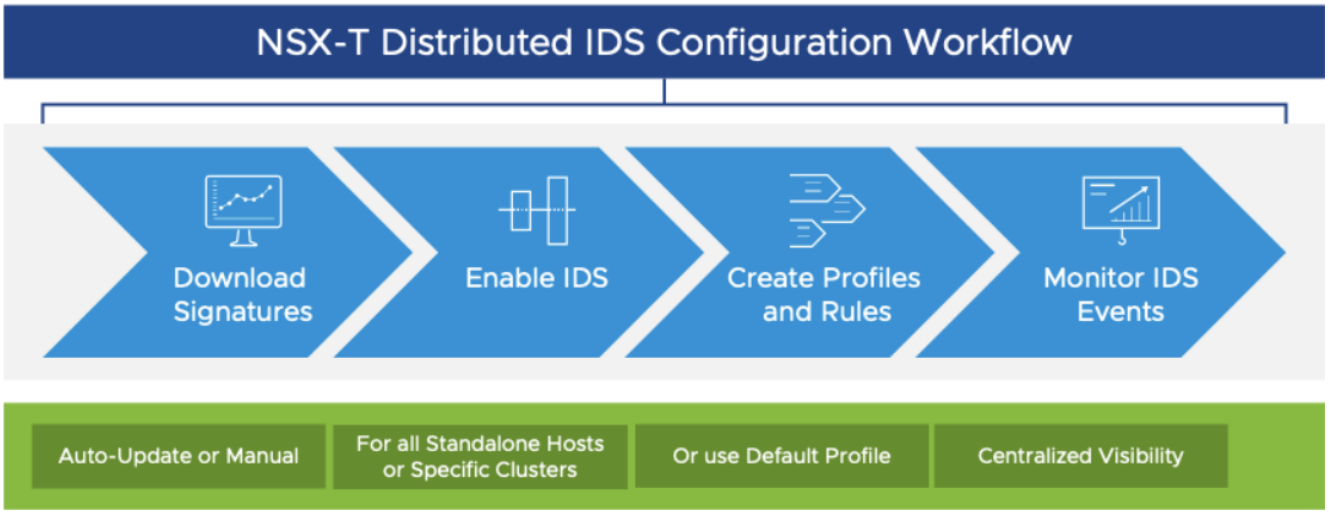

Рис. 3.2. Склад та робочі процеси NSX-T IPS

Налаштування NSX IPS передбачає чотири етапи, як показано на рис. 3.2: завантаження сигнатур, увімкнення IDS, створення профілів та правил та моніторинг подій. Після опису компонентів IPS кожен крок буде детально розглянуто.

Компоненти IPS NSX такі ж, як описані вище для DFW, оскільки функціональність IPS поєднана з DFW. У площині управління Менеджер завантажує оновлення сигнатур IPS із хмарної служби, а користувачі налаштовують профілі та правила IPS. Як і у випадку з DFW, конфігурація передається CCP після збереження в диспетчері. Знову ж таки, як і у випадку з DFW, CCP передає інформацію до LCP на хостах. На хості інформація про сигнатури зберігається у базі даних на хості та налаштовується у шляху до даних. Хост ESXi також збирає дані про трафік та події для передачі менеджеру NSX. На рис. 3.3 показано деталі компонентів IPS всередині хоста.

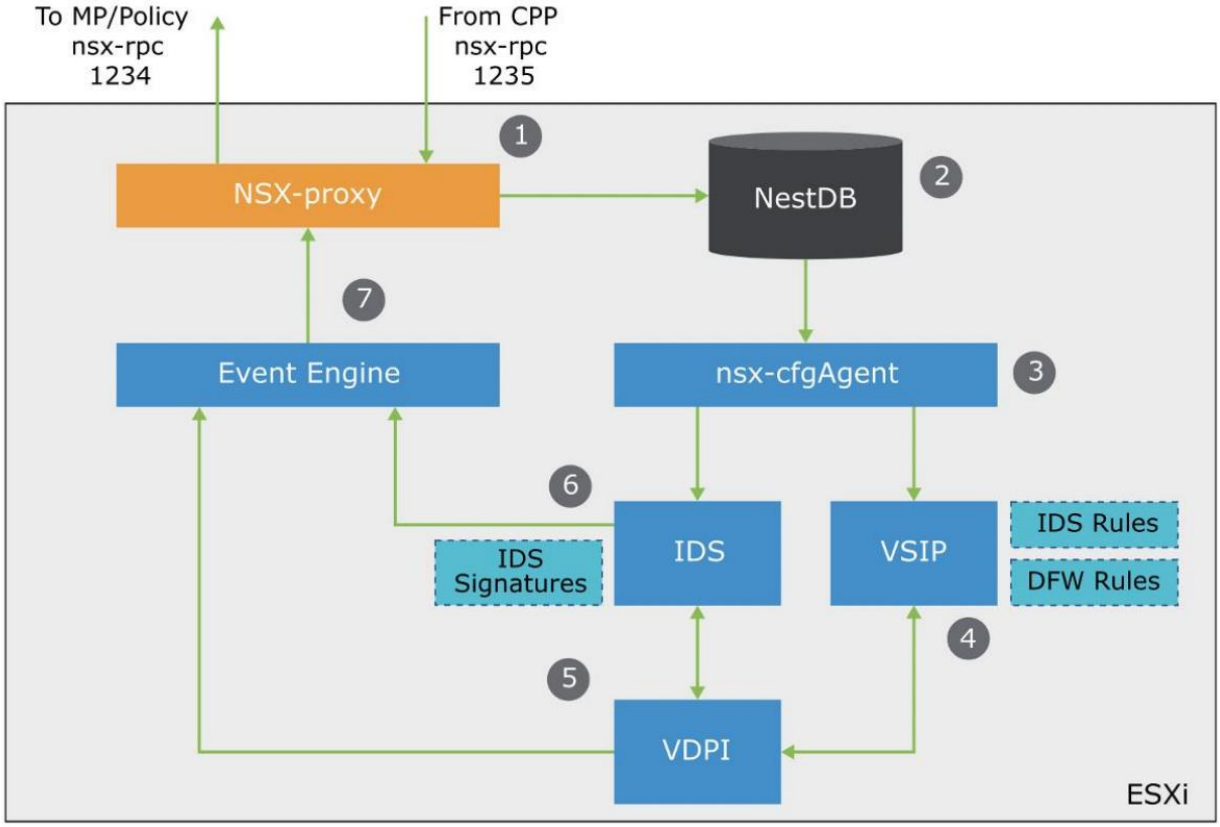

Рис. 3.3. NSX-T IPS компоненти – LCP and host

Коли конфігурація надходить на хост, відбувається наступне.

1. NSX-Proxy отримує зміни конфігурації від CCP і записує дані в NestDB.

2. NestDB зберігає сигнатураи та правила IPS локально.

3. nsx-cfgAgent отримує конфігурацію з NestDB і записує сигнатураи до IPS та правила IPS до VSIP.

4. vSIP оцінює трафік за правилами IPS "цікавого руху". Якщо знайдено збіг, пакет перетворюється на vDPI (Mux)

5. vDPI копіює пакет і надсилає копію через механізм IPS. Пакет звільняється на площині даних vSIP, коли IPS закінчує перевірку

6. Подія IPS генерується механізмом IPS

7. Event Engine збирає метадані потоку та генерує попередження.

Механізм подій – це багатопотоковий механізм (один потік на ядро хосту), розгорнутий на кожному ESXi TN як частина підготовки хосту, що працює в просторі користувача. Цей механізм працює на всіх хостах ESXi незалежно від увімкненого стану IPS. Коли NSX-T інстальовано на хості, на той момент встановлюється все, що потрібно для роботи розподілених IDS/IPS. Ніякого додаткового програмного забезпечення не потрібно надсилати на хост.

Механізм подій оцінює трафік щодо сигнатур IPS лише тоді, коли IPS увімкнено на TN і налаштовано правила IPS. Сигнатури IPS конфігуруються в профілях і програмуються на кожному механізмі IPS. Трафік відображається у профілях, щоб обмежити оцінку сигнатури. Зверніть увагу, що на продуктивність IPS впливає більше перевірений трафік, ніж кількість оцінюваних сигнатур. Набір сигнатур за замовчуванням запрограмований на кожному механізмі IPS, навіть коли IPS вимкнено. У високозахищених середовищах із ізоляцією існує підтримка завантаження оновлень сигнатур в автономному режимі, що передбачає реєстрацію, автентифікацію та завантаження сигнатур у zip-файлі, який потім можна завантажити вручну через інтерфейс користувача [10].

Сигнатури IPS. NSX-T IPS постачає з понад 11 000 сигнатур. В даний час ці сигнатури надає один із найвідоміших постачальників Thread Intelligence, Trustwave, і куратори здійснюються на основі наборів сигнатур Emerging Threat та Trustwave Spiderlabs. Є можливість додавання додаткових постачальників сигнатур.

Signature ID	Details	Product Affected	Attack Target	IDS Severity	CVSS ↓	CVE	Category
4009306	ET EXPLOIT Possible WINS Server Remote Memory Corruption Vulnerability	Windows_DNS_server	DNS_Server	CRITICAL	0.0		

Рис. 3.4. NSX-T IPS сигнатура

Сигнатура (рис. 3.4) складається з багатьох компонентів:

опис та ідентифікатор – вони унікальні для кожної сигнатури – прості рядки або регулярні вирази – вони використовуються для узгодження шаблонів трафіку;

модифікатори – використовуються для виключення пакетів (розмір корисного набору пакетів, порти тощо);

метадані – використовуються для вибіркового ввімкнення сигнатур, які мають відношення до робочого навантаження, яке захищається, використовуючи такі поля для контексту:

постраждалий продукт – широка категорія навантажень, вразливих до експлуатації;

ціль атаки – конкретна служба, вразлива для цієї експлуатації (Drupal Server або Joomla, наприклад);

розгортання.

вплив на ефективність – це необов’язкове поле;

серйозність – інформація, що міститься в більшості сигнатур.

Сигнатури класифікуються на понад 50 категорій/типів, що пояснюють самі собою, включаючи спроби DOS, отримання привілеїв успішного користувача та виявлення shell.code. Кожен тип класифікації має рейтинг типу (1–9) на основі ризику та вірності, пов'язаних з типом події/нападу. Класифікація типу відображається відповідно до рейтингу серйозності IPS NSX (4 - критичний, 3 - високий, 2 - середній та 1 - низький). Серйозність сигнатур допомагає командам безпеки визначати пріоритети інцидентів. Більш висока оцінка вказує на вищий ризик, пов’язаний із вторгненням. Серйозність визначається виходячи з наступного:

серйозність, зазначена в самій сигнатурі;|

оцінка CVSS, зазначена в сигнатурі (відповідно до специфікацій CVSS 3.0);

типовий рейтинг, пов’язаний із класифікаційним типом.

Профілі сигнатур застосовуються до правил IPS через профілі (рис. 3.5). Для відповідного трафіку застосовується єдиний профіль. Набір сигнатур за замовчуванням включає всі критичні сигнатури.

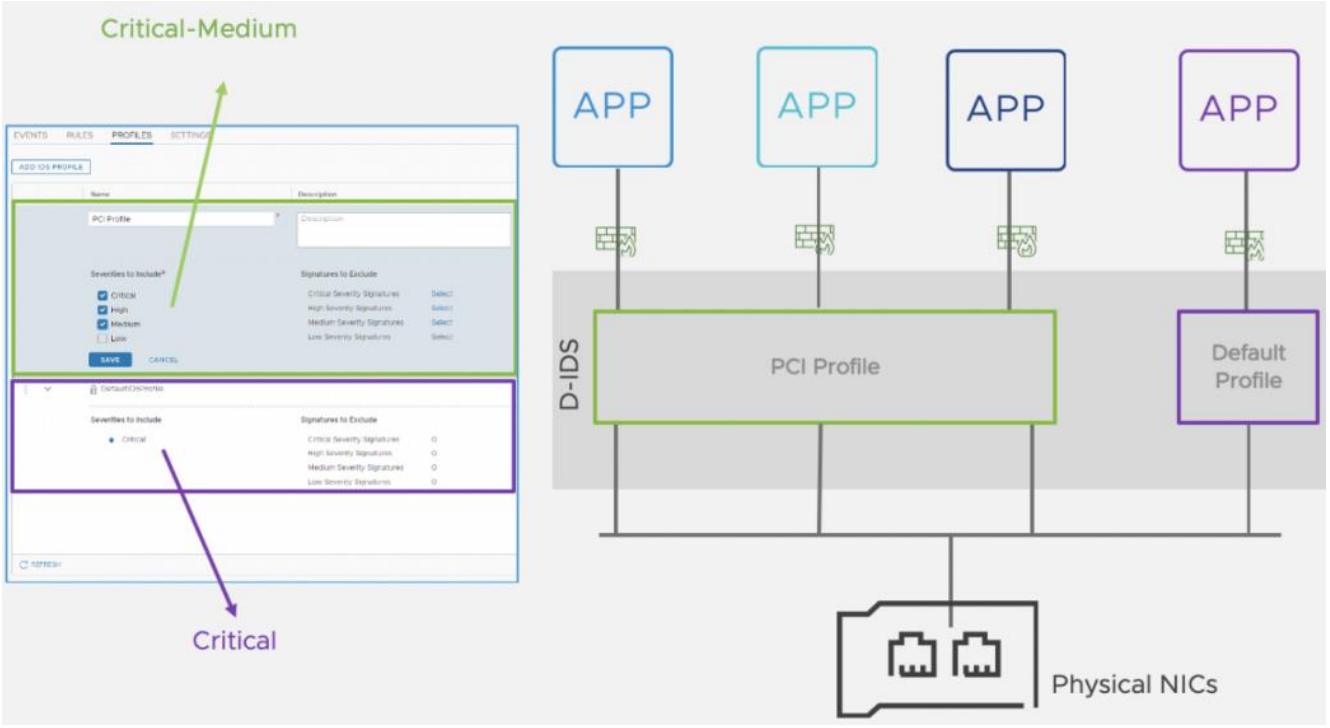

Рис 3.5. NSX-T IPS сигнатурний профіль

Механізм IPS підтримує «орендарів» застосовувати певні профілі до трафіку на vNIC. Це обмежує кількість помилкових спрацьовувань та зменшує вплив на продуктивність. Профілі використовуються в різних стратегіях, таких як один або декілька широких профілів для всього трафіку або багато детальних/конкретних профілів. Треба робити компроміс між адміністративною складністю та надійністю сигнатури робочого навантаження.

Профілі групують сигнатури на основі таких критеріїв:

тип класифікації;

серйозність (критична | висока | середня | низька);

розгортання (Шлюз | DC);

ціль атаки (Клієнт | Сервер);

постраждалий продукт (Web_Browsers | Apache |…);

сигнатури, які можна виключити з профілю.

Для кожного профілю можна встановити виключення для вимкнення окремих сигнатур, які спричиняють помилкові спрацьовування, викликають шум або просто не мають значення для захищених робочих навантажень. Виключення встановлюються для рівня серйозності та можуть бути відфільтровані за

допомогою ідентифікатора сигнатури або метаданих. Перевагами виключення сигнатур є зниження рівня шуму та покращена робота. Якщо виключити занадто багато сигнатур виникає ризик не виявити важливих загроз.

Правила IPS (рис. 3.6) використовуються для відображення профілю IPS до робочих навантажень та трафіку. Іншими словами: правила IPS визначають, що таке «цікавий трафік», який перевіряється механізмом IPS. За замовчуванням правила не налаштовані.

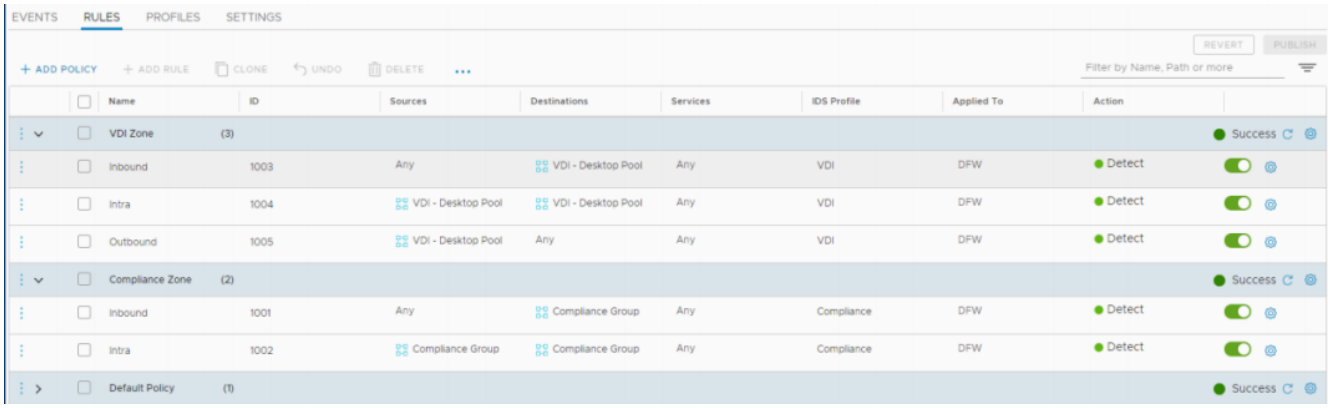

Рис. 3.6. NSX-T IPS Правила

Як видно на рис. 3.6 правила IPS подібні до звичайних правил DFW або правил вставки послуг. Можна вказати один профіль IPS для кожного правила. Правила IPS містять статус і забезпечують підтримку будь-якого типу групи в полях джерела та призначення, як і правила DFW. Однак використання служб L7 APP-ID усередині правил IPS не підтримується. Як було зазначено раніше у DFW, настійно рекомендується використовувати поле Applied-To для обмеження сфери дії правила.

На екрані Огляд безпеки NSX (рис. 3.7) наведено кілька ключових відомостей, які допоможуть командам безпеки. На цьому екрані передбачено три основні інформаційні панелі: Підсумок IPS (для руху на схід-захід), аналіз URL-адреси (для руху на північ-південь) та використання правила DFW.

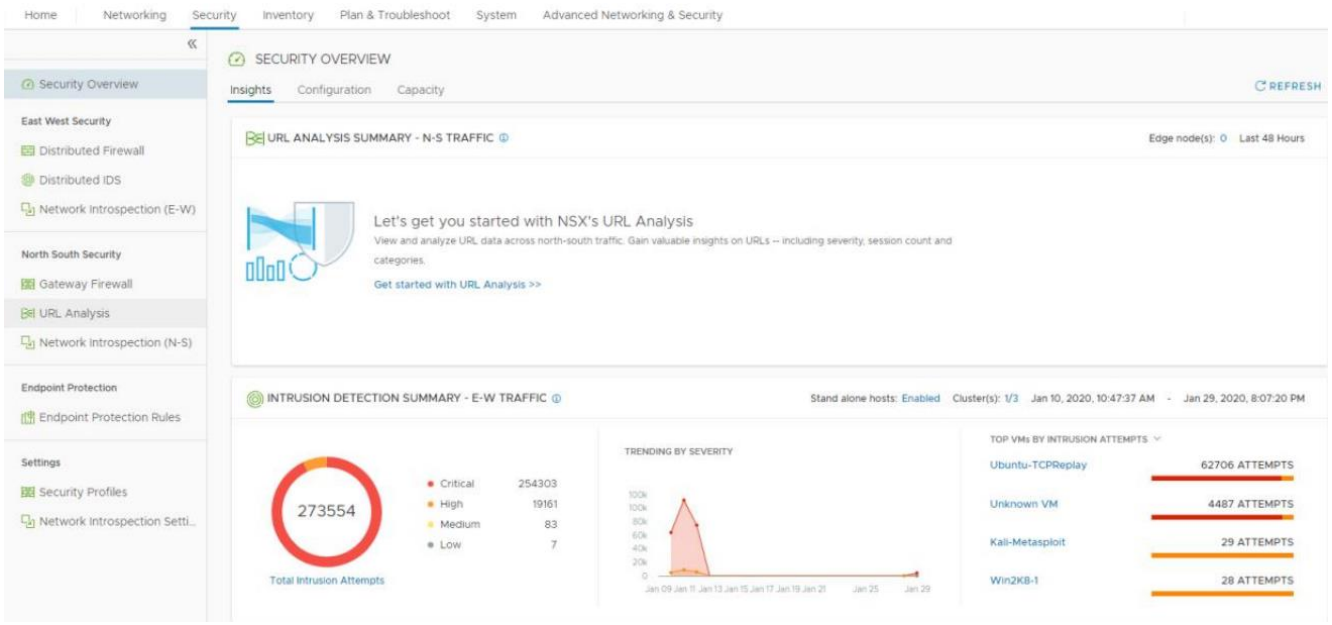

Рис. 3.7. NSX-T IPS Інформаційна панель

Інформаційна панель IPS (рис. 3.7) надає таку інформацію:

увімкнений стан для автономних хостів та кластерів (вгорі показано автономні хости та один з трьох кластерів);

діапазон дат для даних, що відображаються (вгорі показано діапазон дат з 10 січня 2020 року по 29 січня 2020 року);

загальна кількість спроб вторгнення, організованих спроб за ступенем тяжкості (вгорі показано 254303 Критичний, 19161 Високий, 83 Середній та 7 Низький);

тенденція за ступенем серйозності (на рис. вище видно, що був пік 11 січня);

найкращі віртуальні машини за спробами вторгнення або найкращі віртуальні машини за ступенем вразливості (вгорі відображаються найкращі віртуальні машини за допомогою спроб вторгнення).

Вся ця інформація має на меті дати уявлення про стан справ у цілому та вказати, де слід зосередити увагу. Якщо натиснути на загальну кількість спроб вторгнення, ви перейдете на екран Події, показаний на рис. 3.8.

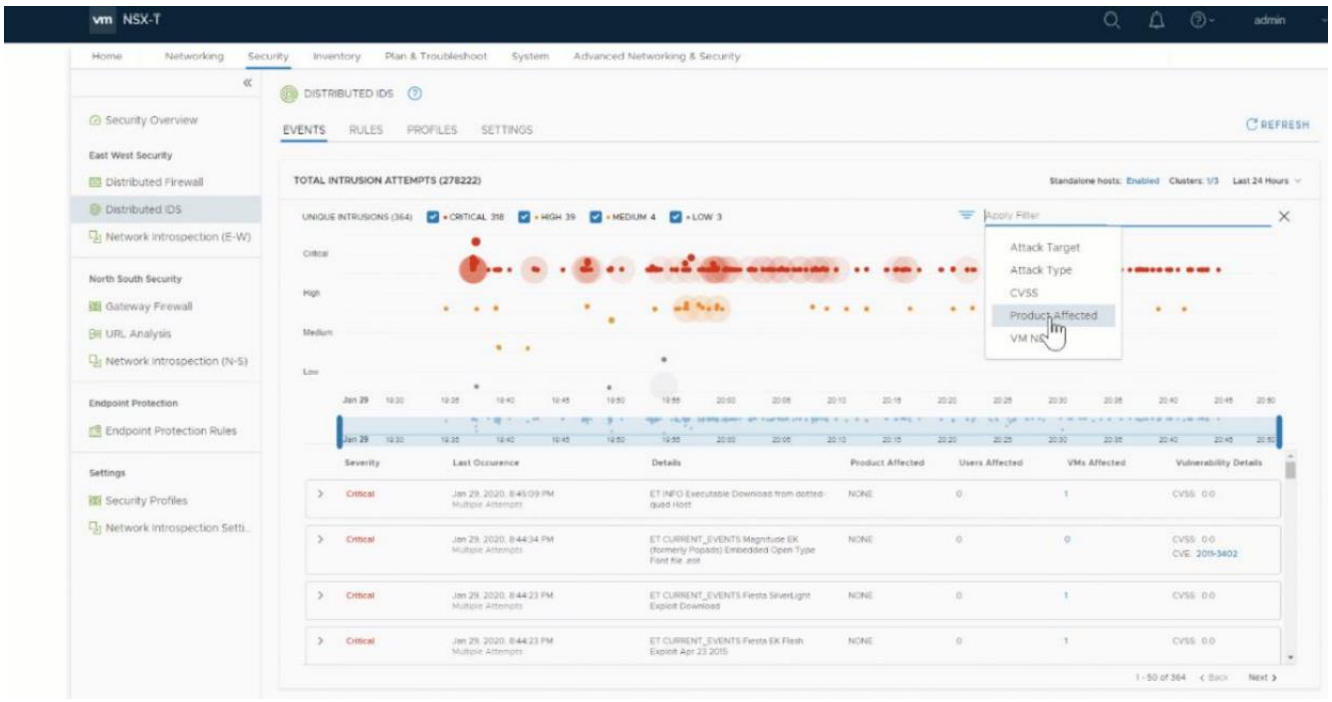

Рис. 3.8. NSX-T IPS Події

Інтерфейс користувача буде містити дані за останні 14 днів або 2 мільйони записів. Праворуч є настроюваний часовий проміжок на 24 години, 48 годин, 7 днів або 14 днів. Кольорові крапки над часовою шкалою вказують на унікальні типи спроб вторгнення. Графік нижче, який можна використовувати для збільшення або зменшення.

Нарешті, деталі події наведені нижче у табличній формі. На кожному рівні серйозності встановлені прапорці для ввімкнення фільтрації. Фільтрування подій може базуватися на:

ціль атаки (сервер | клієнт |…);

тип атаки (троян | Dos | веб-атака |…);

CVSS;

постраждалий продукт;

назва VM.

Кожна подія містить такі деталі:

тяжкість;

опис / деталі;

тип атаки;

ціль атаки (за наявності);

перегляд сигнатури;

постраждалий продукт (за наявності);

деталі вразливості – CVSS (система оцінювання загальної вразливості), ідентифікатор CVE (загальні вразливості та ризики).

На рис. 3.9 нижче показано деталі події.

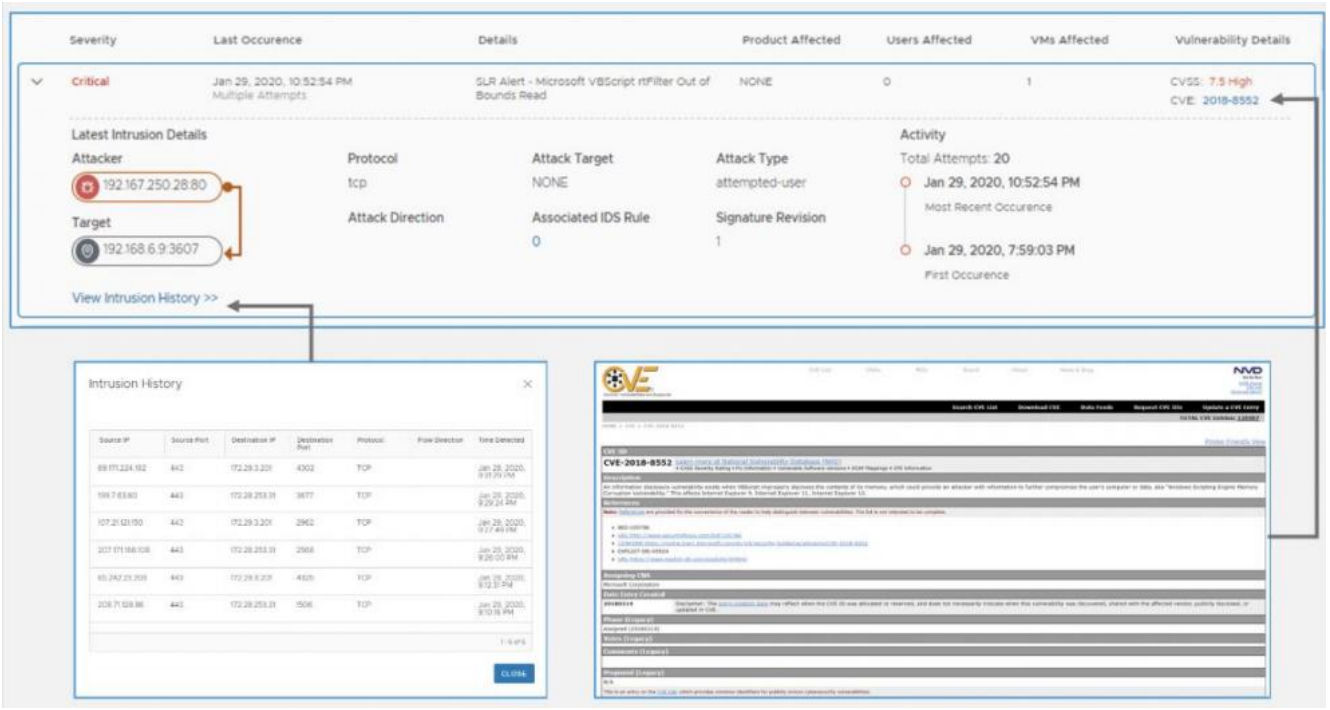

Рис. 3.9. Інформація про події IPS NSX-T

Події можна зберігати на хості за допомогою команди cli для усунення несправностей. За замовчуванням місцеве зберігання подій вимкнено. Коли це ввімкнено, події зберігаються у файлі /var/log/nsx-idps/fast.log.

Як було визначено раніше, робочий процес конфігурації NSX IPS, по суті, складається з чотирьох кроків:

завантаження сигнатури, увімкнення IPS, визначення профілю/правила та моніторинг. Велику частину часу буде витрачено на ітерацію між останніми двома кроками після налаштування розподіленої IPS NSX. Нові завантаження можуть викликати необхідність оновлення профілів та правил, але більшу частину часу буде витрачено на моніторинг. Важливий момент, який слід зазначити стосовно IPS: регулярні DFW, Правила-7 рівня APP-ID та Правила IPS можуть застосовуватися до одного і того ж трафіку, але DFW повинен дозволити передачу DFW через IPS.

Іншими словами, IPS не застосовується до втраченого трафіку.

Хоча NSX IPS можна використовувати в самих різних варіантах використання, *чотири типові випадки використання*: відповідність, створення зон, заміна приладу та обмеження бокової загрози. Хоча вони виділені як чотири випадки індивідуального використання, цілком можливо, що вони співіснують.

Приклад використання IPS: відповідність

NSX IPS зазвичай використовується для забезпечення відповідності програмним IPS для критичних програм, щоб легко досягти вимог відповідності для PCI-DSS, HIPAA, SOX. Багато клієнтів повинні відповідати нормативним вимогам щодо своїх чутливих програм, що стосуються (наприклад) охорони здоров'я або фінансових даних, таких як HIPAA або PCI-DSS.

Ці вимоги дотримання часто визначають потреби в IPS для запобігання крадіжці даних. NSX дозволяє клієнтам легко досягти відповідності нормативним вимогам, дозволяючи мікросегментації зменшити обсяг аудиту та вибірково включивши ISP до робочих навантажень, які повинні відповідати вимогам.

Деякі нормативні вимоги визначають необхідність увімкнення системи виявлення вторгнень для всіх додатків, на які поширюються ці норми. Без NSX IPS це вимагало б, щоб весь трафік проходив через групу приладів, що могло вплинути на архітектуру ЦОД. За допомогою комбінації NSX DFW та NSX IPS трафік може бути мікросегментований та позначений для IPS, як показано на рис. 3.10 нижче.

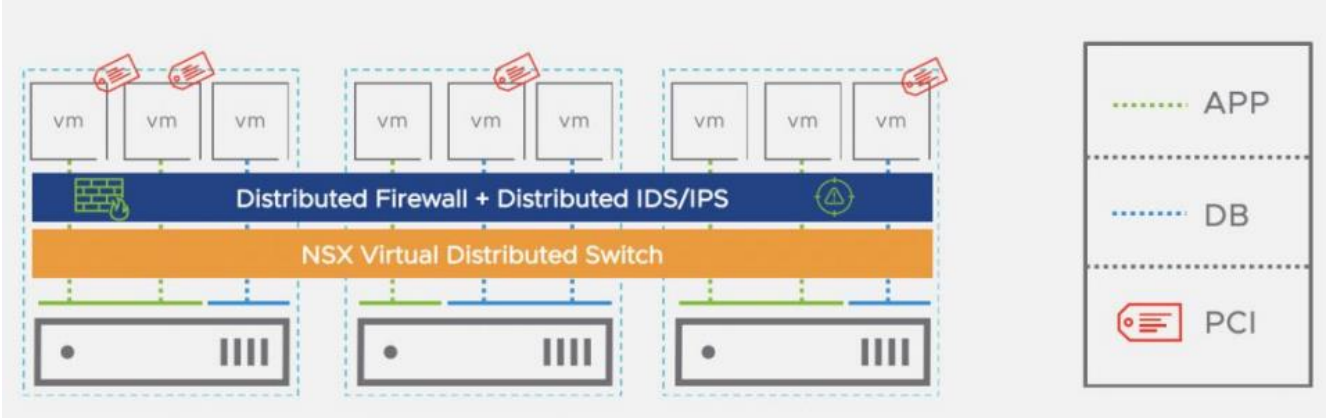

Рис. 3.10. NSX-T IPS Відповідність

У наведеному вище прикладі програма PCI позначена таким чином, щоб вона була брандмауером від інших програм, які є співрезидентами серверного

обладнання. IPS можна застосовувати лише до цієї програми, щоб задовольнити вимоги відповідності, не вимагаючи спеціального обладнання. При бажанні IPS із зменшеним набором сигнатур може застосовуватися, наприклад, лише до частини бази даних інших програм.

Цей приклад використання висвітлює наступні аспекти NSX IPS:

зменшений обсяг відповідності;

вибіркове включення IPS у навколишнє середовище;

застосування сигнатур, що стосуються зони дотримання;

зменшення впливу на продуктивність та попереджувального шуму.

NSX IPS дозволяє клієнтам забезпечувати та доводити відповідність, незалежно від того, де знаходяться робочі навантаження, що дозволяє подальше об'єднання робочих навантажень з різними вимогами до відповідності на x86.

Приклад використання IPS: створення віртуальних зон

NSX IPS дозволяє клієнтам створювати зони в програмному забезпеченні без витрат і складності ізоляції або фізичного розділення. Деякі клієнти надають послуги централізованої інфраструктури для різних напрямків бізнесу або повинні надати зовнішньому партнеру доступ до деяких програм та даних.

Всі клієнти повинні забезпечити належну сегментацію між навантаженнями DMZ, які піддаються зовнішньому / гостьовому Wi-Fi та внутрішнім програмам та даним. Традиційно ця сегментація між орендарями або між DMZ та рештою середовища проводилася шляхом фізичного розділення інфраструктури, тобто робочі навантаження та дані для різних орендарів або різних зон розміщувались на різних серверах, кожен із яких мав свої спеціальні брандмауери.

Це призводить до неоптимального використання апаратних ресурсів. Розподілений брандмауер NSX та розподілена IPS дозволяють клієнтам запускати робочі навантаження, що належать різним орендарям і різним зонам на одних і тих же кластерах гіпервізора, і забезпечують той самий рівень сегментації, який вони отримали б із фізичними брандмауерами та IPS-пристроями, дозволяючи набагато вищі коефіцієнти консолідації.

Приклад використання IPS: заміна приладу

Завдяки додатковій функціональності NSX розподіленої IPS багато клієнтів переходять від застарілих архітектур IPS до приладів до розподілених IPS NSX. Оскільки клієнти віртуалізують свою інфраструктуру центрів обробки даних та мережу, NSX дозволяє їм замінити пристрої фізичної безпеки на внутрішню безпеку, яка вбудована в гіпервізор.

Це здійснюється як для брандмауера з розподіленим брандмауером, так і для IPS із розподіленим IPS та забезпечує єдину політику безпеки для обох у всьому SDDC. Крім того, є реальна економія з точки зору стійки, електроенергії та охолодження завдяки внутрішньому підходу.

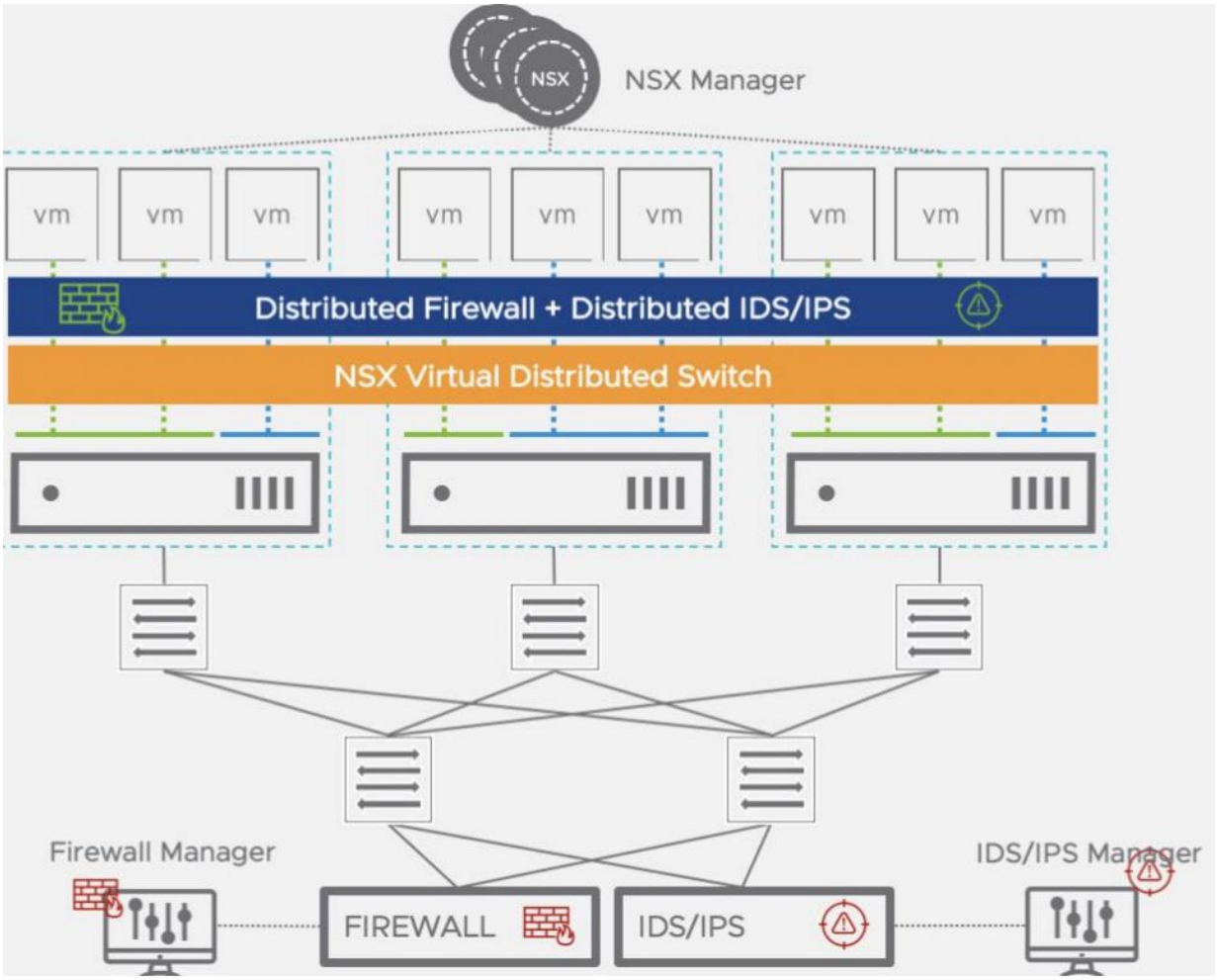

Рис. 3.11. NSX-T NSX distributed IPS заміна приладу

Кожен пристрій безпеки центру обробки даних використовує близько 10 кВт потужності, що становить майже 90 000 кВт на рік на прилад! Коли ці прилади замінюються внутрішньою архітектурою безпеки, яка використовує запасні цикли

кожного центрального процесора в центрі обробки даних, економія швидко збільшується. Економія, яка поставляється з підвищеною поставою безпеки.

Окрім економії приладів безпеки, є значна економія в мережевій інфраструктурі, необхідній для підключення речей, як показано рис. 3.11. Цей лише варіант використання може фінансувати зміну внутрішньої архітектури безпеки.

Приклад використання IPS: виявлення бічних загроз

NSX IPS дозволяє клієнтам поєднувати виявлення на основі сигнатур, виявлення аномалій та перевірки відповідності протоколу. Майже незмінно, фактична мета атаки не така, як зловмисник, який спочатку отримав доступ. Це означає, що зловмисник намагатиметься рухатись навколишнім середовищем, щоб викрасти цінні дані, які він шукає (рис. 3.12).

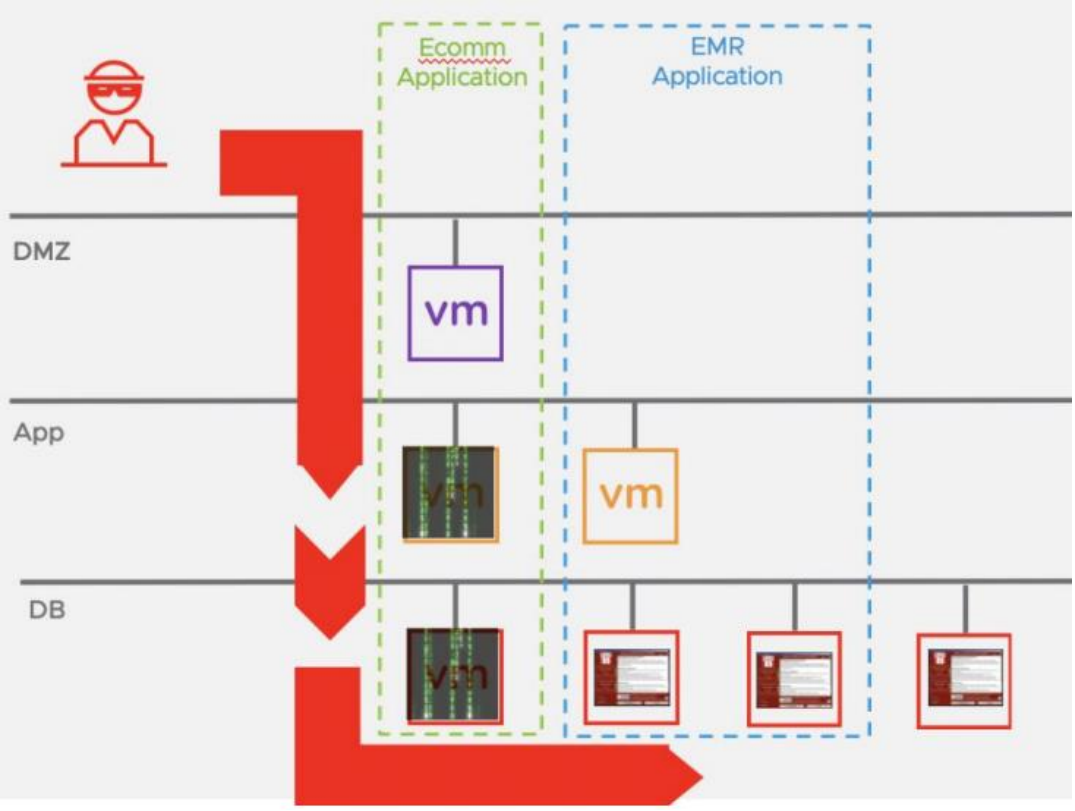

Рис. 3.12. NSX-T Бічний рух загрози

Отже, вміння не просто захищатись від початкового вектора атаки, а й проти бічного руху є критичним. Мікросегментація за допомогою розподіленого брандмауера є ключовим фактором зменшення поверхні атаки та значно ускладнює бічний рух. Тепер мікросегментація вперше стає оперативно можливою для інтерфейсу кожного робочого навантаження за допомогою служби виявлення та

запобігання вторгненню для виявлення та блокування спроб використання вразливих місць, де б вони не існували.

Цей захист існує незалежно від того, чи намагається зловмисник отримати початковий доступ у середовищі, чи вже порушив робоче навантаження на тій самій VLAN і зараз намагається перейти в бік до цільової бази даних на цій самій VLAN.

Розподілене IPS-фронтальне кожне робоче навантаження дозволяє виявляти експлойт незалежно від того, що це початковий вектор атаки, бічне поширення або ексфільтрація.

3.2. Рекомендації щодо застосування технології виявлення та попередження вторгнень в інформаційну систему підприємства

Частота і витонченість атак ростуть безпрецедентними темпами, і компанії більше не можуть покладатися на традиційні методи забезпечення безпеки для внутрішньої мережі. Вони повинні інвестувати в правильні можливості для захисту внутрішніх мереж прямо зараз, тобто їм необхідно використовувати правильний інструмент для роботи [4].

Однак дотримання правильного балансу між охопленням і простотою має вирішальне значення для професіоналів в області безпеки. Щоб впоратися з цими зростаючими проблемами, Forrester рекомендує наступне [4]:

встановіть стратегію виживання. Кіберпростір – це зона бойових дій. Це означає, що кожен пакет, що відправляється вашим бізнесом і клієнтами, активно проходить через поле битви. Спроба перетнути це поле битви без дієвої стратегії – гарантія того, що рано чи пізно ваша організація стане жертвою. Визначте стратегію і приведіть в дію план виживання, і нехай ваш план буде визначати ваш вибір технологій;

Zero Trust (нульова довіра) вимагає детального контролю безпеки. Додатки та мережі існують всюди в сьогоднішньому технологічному ландшафті. Організації потребують детальних політик безпеки для всієї інфраструктури і аж до рівня робочих навантажень, щоб виключити сліпі плями. Повний набір детальних

елементів управління може дозволити отримати перевагу в цьому динамічному середовищі;

огляньте більше трафіку сервер-сервер. Щоб зменшити поверхню атаки, видиму для потенційних зловмисників, перевіряйте весь трафік сервер-сервер. Перевірка трафіку сервер-сервер дозволяє на ранній стадії виявити бічний рух і знизити збиток. По можливості вибирайте інструменти перевірки, які не вимагають перепроектування мережі, але мінімізують вплив на мережу. Рухайтеся зі швидкістю розробки додатків;

швидкість розробки додатків створила серйозну проблему для груп безпеки, що працюють з традиційними архітектурами безпеки на основі пристроїв. Щоб розробники не пішли на компроміс щодо безпеки на користь швидкості, виберіть елементи управління безпекою програмного забезпечення, які відстежують життєвий цикл програм, є автоматизуються і можуть інтегруватися з системами оркестровки;

необхідно спросити як стек безпеки, так і операції. Завдяки інноваціям за останні кілька років стало можливим отримати просте, але надійне рішення безпеки. Шукайте рішення, вбудовані в інфраструктуру, щоб спростити забезпечення безпеки і управління. Простота дозволяє узгоджено застосовувати заходи безпеки, обмежуючи при цьому неправильну конфігурацію.

Десять (або так) найкращих практик внутрішнього брандмауера [6]:

Впровадження будь-якого нового підходу до безпеки вимагає часу та зусиль команди безпеки. З цієї причини, хоча захист горизонтального мережевого трафіку простіший і швидший за допомогою розподіленого внутрішнього брандмауера, більшість організацій воліють застосовувати поетапний підхід для покращення безпеки центрів обробки даних.

Окрім того, щоб не перевантажувати команду безпеки значною ініціативою, розбиття внутрішньої брандмауера на менших проектах приносить і інші переваги: це дозволяє командам безпеки довести успіх на ранніх стадіях та продемонструвати цінність підходу для внутрішніх зацікавлених сторін.

Потім вони можуть вибрати, спираючись на свій досвід, розширити використання розподіленого внутрішнього брандмауера, набираючи оперативної зрілості, швидкості та впевненості в процесі прогресу. Наступні кроки були використані клієнтами VMware, щоб почати з малого, а потім постійно посилювати захист своїх центрів обробки даних:

макросегментація мережі;

мікросегментація кожного додатку;

додавання та застосування IDS/IPS;

захист додаткових добре зрозумілих програм;

забезпечення видимості горизонтального мережевого трафіку;

захист усіх критичних програм;

захист усіх додатків;

розгортання та застосування розширеної IDS/IPS;

розширення за межами віртуалізованого центру обробки даних;

захист нових програм перед розгортанням;

застосування попереднього полювання на загрози.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми виявлення та попередження вторгнень в інформаційну систему підприємства.

Вважається, що використання традиційних міжмережевих екранів периметра для захисту внутрішньої мережі неефективно та необхідно застосовувати методи та засоби виявлення та попередження вторгнень в інформаційну систему підприємства.

Проведено аналіз існуючих технологій виявлення та попередження вторгнень в інформаційну систему підприємства та встановлено що найбільш перспективним є застосування технології IPS.

Системи виявлення й запобігання вторгненням в першу чергу орієнтовані на виявлення можливих інцидентів, реєстрацію інформації про них, спробу їх зупинити і повідомити про них адміністраторів безпеки. Крім того, організації використовують IPS для інших цілей, таких як виявлення проблем з політиками безпеки, документування існуючих загроз і утримання людей від порушення політик безпеки.

Досліджено технологію виявлення та попередження вторгнень в інформаційну систему підприємства на прикладі рішення VMware NSX Distributed IDS/IPS. Рішення VMware NSX Distributed IDS/IPS надає адміністраторам безпеки програмне рішення IDS/IPS, яке дозволяє їм забезпечувати відповідність нормативним вимогам, створювати віртуальні зони і виявляти бічне переміщення загроз в горизонтальному трафіку.

Основними перевагами рішення VMware NSX є:

гнучка пропускна здатність, яка полягає в усуненні вузьких місць в обладнанні за рахунок можливості перевірки, що автоматично масштабується з кожним робочим навантаженням;

спрощена мережева архітектура, яка сприяє уникненню необхідності направляти трафік на централізовані пристрої і зменшенню перевантаження мережі

за допомогою повністю розподіленої архітектури;

зменшення кількості помилкових спрацьовувань – більше робочих навантажень з нульовим кількістю помилкових спрацьовувань з ретельно підібраними наборами правил і більш точною відповідністю сигнатур на основі точного контексту програми;

підвищення ефективності використання ємності, сутність якого полягає у повторному використанні існуючих невикористаних обчислювальних ресурсів, усуваючи необхідність в додатково виділених пристроях.

Розглянуто порядок втілення та застосування технології виявлення та попередження вторгнень в інформаційну систему підприємства на прикладі рішення VMware NSX Distributed IDS/IPS.

Розроблено рекомендації керівникам підприємств та фахівцям з кібербезпеки щодо вибору та застосування системи попередження вторгнень в інформаційну систему підприємства.

Від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів виявлення та попередження вторгнень та ефективного їх застосування залежить ефективність забезпечення кібербезпеки інформаційних систем підприємства.

Таким чином, запропоновані в роботі рекомендації мають сприяти підвищенню захищеності функціонування інформаційної системи підприємства шляхом втілення та застосування технології виявлення та попередження вторгнень.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2020 Data Breach Investigations Report. Verizon [Електронний ресурс] – Режим доступу: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf.

2. To Enable Zero Trust, Rethink Your Firewall Strategy. Forrester Consulting [Електронний ресурс] – Режим доступу: https://www.vmware.com/content/dam/learn/en/amer/fy21/pdf/482143_VMware_Forrester_SDF.pdf.

3. Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft). Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Peter Mell. National Institute of Standards and Technology Special Publication 800-94 Revision 1 (Draft), 111 pages (Jul. 2012) https://csrc.nist.gov/csrc/media/publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf.

4. Five Critical Requirements for Internal Firewalling in the Data Center. White Paper – March 2020. VMware [Електронний ресурс] – Режим доступу: https://www.vmware.com/content/dam/learn/en/amer/fy21/pdf/492966_Five_Critical_Requirements_for_Internal_Firewalling_in_the_Data_Center.pdf

5. Professional Services for Virtual Cloud Network [Електронний ресурс] – Режим доступу: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmw-professional-services-for-virtual-cloud-network-solution-overview.pdf

6. Internal Firewalls For Dummies. VMware Special Edition by R. Dube [Електронний ресурс] – Режим доступу: https://www.vmware.com/content/dam/learn/en/amer/fy21/pdf/656351_Internal-firewalls-ebook.pdf

7. VMware NSX Distributed IDS/IPS. Enhancing VMware Service-defined Firewall with advanced threat detection [Електронний ресурс] – Режим доступу: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-distributed-ids-ips-solution-overview-dec.pdf

8. NSX-T Distributed IDS/IPS Configuration. Peter Milchov [Електронний ресурс] – Режим доступу: https://virtualination.com/NSX/nsx-t-distributed-ids-ips-configuration

9. NSX-T 3.0 - Distributed IDS/IPS Proof of Value Guide [Електронний ресурс] – Режим доступу: https://github.com/vmware-nsx/eval-docs-ids-ips

10. NSX-T Security Reference Guide. Version 1.0. December 1, 2020 [Електронний ресурс] – Режим доступу: https://communities.vmware.com/wbsdv95928/attachments/wbsdv95928/4002/279/1/NSX%20Security%20Reference%20Guide.pdf.

11. Колотухін Денис Вадимович. Технологія розподіленого виявлення та попередження вторгнень в інформаційну систему підприємства. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій. 27 жовтня 2021. Тези доповідей. С. 28 – 30. http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)